



AN AJEEVI EBOOK

Integrated Command & Control Centers

A practical guide to planning, building and
running an integrated command and control center

Connect. Coordinate. Command.

ABOUT THIS EBOOK

Read this first

A practical guide for the people who plan, build and run the command centers that keep cities safe and smart.

WHO IT IS FOR

City commissioners and municipal teams, smart city special purpose vehicles, police and traffic authorities, utilities, emergency services, facility managers, consultants and system integrators. No technical background is needed. Each chapter explains ideas in plain language and ends with practical steps.

HOW TO USE IT

- Read Part One to understand the foundations: what an integrated command and control center (ICCC) is, how it is built and where it should run.
- Use Part Two as a catalog. It describes ten capabilities, one per page, so you can read only the ones that matter to you.
- Use Part Three to plan: AI agents, people and procedures, security and privacy, a phased roadmap, governance and measuring success.
- Already running an ICCC? Go straight to Chapter 11 for a health check, then return to the chapters that match your gaps.
- The contents page and the PDF bookmarks link to every chapter.

A NOTE ON EXAMPLES AND PRODUCTS

This ebook gives general guidance. Every city is different, so adapt the ideas to your laws, budgets and priorities. Product names such as GyanKendram, GyanAkshi and TransAJV refer to AJEEVI Technologies platforms. Measures and timelines are illustrative, not targets or guarantees.

ABOUT THIS EDITION

Integrated Command & Control Centers. First edition, 2026. Published by AJEEVI Technologies.

© 2026 AJEEVI Technologies. All rights reserved. You may share this ebook in its complete form. Please do not alter it or sell it. All trademarks belong to their respective owners.

CONTENTS

What is inside

	Read this first	2
	Introduction: Why a city needs one place to see and act	4
	Our approach: Connect. Coordinate. Command.	5
PART ONE	Foundations	6
1	What is an ICCC?	7
2	The ICCC architecture	8
3	Data and integration	9
4	Deployment and resilience	10
PART TWO	Ten key capabilities	11
01	Unified operations dashboard and city map	12
02	Video wall and video management	13
03	Alert rules, correlation and escalation	14
04	Incident management and dispatch	15
05	Field force and mobile response	16
06	Emergency and multi-agency coordination	17
07	Traffic and mobility command	18
08	Utility and environment monitoring	19
09	Citizen engagement and helpdesk	20
10	Analytics, reporting and digital twin	21
PART THREE	Making it real	22
5	AI agents in the command center	23
6	People, SOPs and the operating model	24
7	Security, privacy and trust	25
8	A phased roadmap	26
9	Governance, procurement and operations	27
10	Measuring success	28
11	Common pitfalls and a readiness checklist	29
	Glossary	30
	About AJEEVI	31

INTRODUCTION

Why a city needs one place to see and act

Cities already own many systems: cameras, signal controllers, water meters, fire panels, helpdesks and radios. Each one tells part of the story. A broken signal, a flooded underpass, a crowd at a station and a stream of citizen complaints may all describe the same afternoon, yet each lands on a different screen in a different office. Coordination then depends on phone calls, and phone calls are slow when minutes matter.

An integrated command and control center (ICCC) is where those signals meet. It is the place where a city sees what is happening, decides what to do and directs the response across departments. Many Indian cities have built one under the Smart Cities Mission and similar programs. The next challenge is to make each one trusted, used every day and central to how the city runs.

THE IDEA IN ONE LINE

An ICCC is not a room full of screens. It is one picture, shared rules and clear ownership, working around the clock.

THREE SHIFTS THAT MAKE THIS POSSIBLE

- **From many screens to one picture.** Video, sensors, helpdesk and field teams feed one platform and one map, so every department sees the same facts.
- **From phone calls to workflows.** Alerts become incidents with an owner, a timer and a record, instead of messages that can be missed.
- **From reports to real-time decisions.** Data becomes alerts, recommendations and simulations that help people choose what to do next, and then helps them learn afterwards.

WHY NOW

Cameras, sensors and connectivity have become affordable. AI can read video and sensor data at a scale no control room could handle manually. Cloud, edge and on-premise options give cities control over where their data lives. The question is no longer whether to build a command center. It is how to make one that people use, trust and keep improving.

This ebook is written for that question. It is practical rather than theoretical, and it focuses on capabilities that cities can start with today, whether they are planning a first ICCC or getting more from an existing one.

INTRODUCTION

Our approach: Connect. Coordinate. Command.

Three verbs describe what a good command center does all day.

Step	What happens	Example
Connect	Cameras, sensors, city systems and teams are linked to one platform through open interfaces.	A camera feed, a flow meter alarm and a helpdesk ticket appear on the same map.
Coordinate	Events are correlated, ranked and routed to the right department by shared rules and SOPs.	A flood alert reaches the traffic team, the drainage team and the helpdesk at once.
Command	Authorized people decide, direct field teams and track every incident to closure.	A supervisor reassigns a team and the incident closes with photo proof.

FIVE PRINCIPLES USED THROUGHOUT THIS BOOK

- **Operations first, technology second.** Define the daily decisions the center must support, then choose the tools. Every capability in Part Two begins with a challenge and ends with measures.
- **One platform, many departments.** Share the map, the incident queue, the data and the command floor, so each new department costs less to add than the last.
- **Open and interoperable.** Prefer open standards and open APIs, so systems from different suppliers can work together and the city is not locked in.
- **People stay in the loop.** Software recommends and automates routine steps. Trained people make the important decisions.
- **Resilient by design.** The center must keep working when a network, a power feed or a whole site fails, because that is when it is needed most.

ADVICE FROM THE FIELD

Begin with one shared incident queue and a few agreed SOPs. A center that handles three kinds of incidents well earns the trust to take on thirty.

01

PART ONE

Foundations

What an ICCC is, how it is built, what it connects to and where the software should run.



PART ONE | CHAPTER 1

What is an ICCC?

A facility, a platform and a way of working that brings city operations together.

An integrated command and control center is the place where a city sees what is happening, decides what to do and directs the response across departments. It is better understood by what it is made of than by the screens on its wall. Four components matter.

Component	What it means	Examples
Facility	The command floor where teams work, plus a crisis room and a backup site.	Video wall, operator consoles, meeting room, power and cooling
Platform	Software that connects systems and turns data into alerts, incidents and reports.	Integration layer, GIS map, rules engine, incident workflow, dashboards
People	Trained teams who watch, decide and coordinate.	Operators, shift supervisors, department liaisons, analysts
Process	Written rules for who does what, and when.	SOPs, escalation paths, service levels, review meetings

FOUR LEVELS OF MATURITY

Level	What it looks like	Typical sign
1 Monitor	Screens show live feeds, but each department still works alone.	Many screens, few shared actions
2 Integrate	Data from several systems sits on one platform and one map.	One shared incident queue
3 Coordinate	SOP-driven workflows run across departments.	Handoffs tracked, targets measured
4 Anticipate	Analytics, simulation and AI agents help predict and recommend.	Problems prevented, not only handled

WHAT AN ICCC IS NOT

- **Not only a video wall.** Screens are the visible part. The value lies in the rules, workflows and people behind them.
- **Not a replacement for departments.** Departments still own their field work. The center coordinates and keeps the record.
- **Not a one-time project.** It needs operations, maintenance and continuous improvement, with clear owners.
- **Not only for emergencies.** Its daily value comes from routine work: lamps, leaks, blockages, complaints and events.

PART ONE | CHAPTER 2

The ICCC architecture

Five layers turn raw signals into coordinated action, and a feedback loop keeps improving them.



REVIEW: results feed back to improve rules, models, SOPs and plans

Layer	Role	Typical components
Sources	Observe the city and capture data.	Cameras, air and noise sensors, flow and pressure meters, lamp controllers, signal controllers, fire panels, emergency calls
Integrate	Bring data from many systems into one place, reliably and securely.	Camera and device connectors, gateways, message broker, open APIs, data platform
Correlate	Clean, link and analyze events.	Rules engine, AI video analytics, time-series analytics, GIS maps, duplicate merging
Coordinate	Turn events into owned, tracked work.	Incident management, SOP workflows, escalation, dispatch, event rooms
Command	Give people the right view and the means to act.	Video wall, role-based dashboards, mobile apps for field teams, device control, citizen notifications

Review closes the loop. Every incident, ticket and measurement is a data point. Reviewing results lets teams tune thresholds, retrain models, update SOPs and decide where to invest next.

DESIGN RULE

Choose layers that fit together. Cameras and sensors from different makers should connect through standard interfaces to one platform, not to a separate screen each.

AJEEVI builds across these layers: rugged IoT devices (GyanYantram), AI video analytics (GyanAkshi), the integrated command center platform (GyanKendram) and the sector platforms built on them.

PART ONE | CHAPTER 3

Data and integration

An ICCC is only as good as the data and systems that flow into it.

Most cities already own useful systems. The practical task is to bring them together without replacing everything. This is integration, and it is usually where ICCC projects succeed or stall.

Data source	Examples	How it commonly connects
Video	Street, junction and building cameras; video management systems	Camera streams such as RTSP; interoperability through ONVIF
IoT sensors	Air, noise, water level, rainfall, bin fill, lamp controllers	Low-power networks, cellular, gateways, MQTT or HTTP APIs
Building systems	HVAC, lighting, meters, fire panels, access control	BACnet, Modbus and vendor APIs through gateways
Utility and traffic systems	SCADA, signal controllers, flow meters, parking	Standard protocols such as OPC UA and Modbus, and secure APIs
Emergency and telephony	Emergency calls, dispatch software, radio	CAD interfaces, SIP and vendor APIs
People and operations	Helpdesk calls, apps, field job updates, social media	Web and mobile apps, call-center integration
Maps and external feeds	GIS layers, weather, public transport, event calendars	Map services, open data feeds, secure APIs

INTEGRATION PRINCIPLES

- **Integrate, do not rip and replace.** Connect existing systems where possible and replace only what cannot be connected.
- **Use open interfaces.** Require documented APIs and standard protocols in every tender, so new vendors can plug in.
- **One event model.** Give every asset, location and event a consistent identity and format, so alerts can be linked on a map and across departments.
- **Integrate by value.** Rank systems by the decisions they support, connect the most valuable first and test each one against a real scenario.
- **Plan for data quality.** Calibrate sensors, check for gaps and flag bad readings, because poor data produces poor alerts.
- **Respect data ownership.** The city owns its data. Contracts should say so, including how data is exported at the end.

PROCUREMENT TIP

If a camera, sensor or system cannot share its data, it cannot help the city. Make open interfaces a condition of purchase.

PART ONE | CHAPTER 4

Deployment and resilience

Where the software runs affects speed, cost, control of data and whether the center survives a bad day.

Option	What it means	Good fit when	Consider
Edge	Analytics run next to the camera or sensor.	Fast alerts are needed or bandwidth is limited.	Device management and updates across many sites.
On-premise	Servers sit in a city-owned data center or command center.	Data must stay inside the city or agency.	Capital cost, space, power and skilled operators.
Private or government cloud	A dedicated cloud environment inside national boundaries.	You want scalability with local control.	Provider approval, data residency and exit terms.
Public cloud	Shared infrastructure from a commercial provider.	Workloads are not sensitive and need to scale quickly.	Data residency rules and costs that grow with use.
Hybrid	A mix of edge, on-premise and cloud.	Different workloads have different needs.	Needs clear architecture and monitoring.

RESILIENCE FOR A 24x7 CENTER

- **Power.** Provide UPS and generator backup for the command floor, servers and network equipment, and test them.
- **Network.** Use at least two independent paths to critical sites, and keep working views of key cameras if one path fails.
- **Backup site.** Keep a disaster recovery (DR) site or a backup control room, with agreed recovery time and data-loss limits.
- **Failover drills.** Rehearse switching to the backup, not just on paper. Untested failover is a hope, not a plan.
- **Graceful degradation.** Decide which functions must work offline, such as dispatch, and how teams continue if the platform is down.

SOVEREIGN AND AIR-GAPPED AI

Some agencies need AI that runs entirely inside their own boundaries, with no data leaving the premises. Sovereign AI means models and data are hosted and controlled in-country, on-premise or in an air-gapped environment. It lets sensitive uses such as public safety use AI without sending video to outside services. AJEEVI supports in-country and on-premise deployments for this reason.

RULE OF THUMB

Decide where the data lives, and what must keep working when something fails, before you decide which software to buy.

02

PART TWO

Ten key capabilities

Ten practical capabilities, one page each: the challenge, how it works, what teams gain and how to measure it.



USE CASE 01 OF 10

Unified operations dashboard and city map

See the whole city, then drill down to the one asset that matters.

THE CHALLENGE

Each department sees only its own data. Senior officers rely on phone calls and daily reports to learn what is happening in the city right now.

HOW IT WORKS

All connected systems feed one map-based operational view. Layers for cameras, sensors, incidents, field teams and assets can be switched on and off. Role-based dashboards give each department what it needs, while a city-level view shows the whole picture.

- Map with layers for assets, events and teams
- Role-based dashboards for each department and level
- Live status of devices, networks and field teams
- Drill-down from city to ward to single asset
- Saved views for events, festivals and emergencies

WHAT TEAMS GAIN

- One shared picture across departments
- Quicker briefings for senior officers
- Fewer calls to find out what is happening

METRICS TO TRACK

- Share of connected systems live
- Active dashboard users per week
- Data delay from source to screen
- Time to brief officers during an event

PRACTICAL TIP

Show fewer, better indicators on the main screen. A dashboard that tries to show everything ends up showing nothing.

USE CASE 02 OF 10

Video wall and video management

Turn thousands of camera feeds into the few views that matter right now.

THE CHALLENGE

A city may have thousands of cameras from many makers. Operators can watch only a few screens at once, and finding footage after an incident can take hours.

HOW IT WORKS

A video management layer pulls streams from cameras of different makes through standard interfaces. The video wall shows cameras selected by alerts, location or operator choice, and AI analytics decide which cameras deserve attention.

- Integration of existing cameras through ONVIF and RTSP
- An alert-driven video wall that brings up the relevant camera
- Camera health monitoring and fault tickets
- A searchable archive by time, place and event type
- Retention rules and role-based access with audit logs

WHAT TEAMS GAIN

- Operators focus on events, not walls of screens
- Faster evidence retrieval
- Early detection of failed cameras

METRICS TO TRACK

- Camera uptime
- Time to retrieve footage
- Share of cameras with analytics running
- Alert-to-acknowledge time

PRACTICAL TIP

Check camera health every day. A camera that has been down for weeks is worse than none, because people assume it is watching.

Alert rules, correlation and escalation

Fewer, better alerts, and a guarantee that important ones are never ignored.

THE CHALLENGE

Alerts arrive from many sources. Without rules, operators drown in noise, duplicates and false alarms, and a genuine emergency can be missed.

HOW IT WORKS

A rules engine receives events, removes duplicates, links related events, such as a camera detection and a sensor alarm at the same place, and sets severity. Escalation rules notify a supervisor when nobody acts within a set time.

- Alert intake from video, sensors, systems and calls
- Duplicate merging and event correlation
- Severity levels and priorities agreed with departments
- Time-based escalation paths
- A change log for every rule, with review dates

WHAT TEAMS GAIN

- Fewer and more meaningful alerts
- Important events reach the right person first
- Consistent handling on every shift

METRICS TO TRACK

- Alerts per operator per hour
- False alert rate
- Share of alerts escalated on time
- Share of alerts acted on

PRACTICAL TIP

Review the ten noisiest rules every month, then tune, merge or retire them. Alert fatigue is the quiet failure of many command centers.

USE CASE 04 OF 10

Incident management and dispatch

Give every incident an owner, a clock and a record.

THE CHALLENGE

Incidents are handled through calls and messages. Ownership is unclear, minor tasks compete with serious ones and records are scattered.

HOW IT WORKS

Every incident is a record from detection to closure. The platform suggests the responsible team by type and location, notifies it, tracks acknowledgement and keeps the incident open until it is closed with notes.

- Incident creation from alerts, calls and apps
- Classification, severity and routing by SOP
- Dispatch with location and context
- Live status, timers and escalation
- Closure notes and a complete incident history

WHAT TEAMS GAIN

- Clear ownership of every incident
- Faster response and fewer dropped tasks
- A full history for review and training

METRICS TO TRACK

- Time to assign
- Time to arrive on site
- Time to resolve
- Share of incidents closed within target

PRACTICAL TIP

Hold a monthly review of the five slowest incidents. They show exactly where procedures and handoffs need fixing.

USE CASE 05 OF 10

Field force and mobile response

Keep the command center and the person on the street looking at the same job.

THE CHALLENGE

A command center loses sight of a team once it leaves the base. Updates arrive late by phone, and proof of work is thin.

HOW IT WORKS

Field staff use a mobile app to receive tasks, find the location, update status and add photos and notes. Supervisors see team availability and workload on the map, and the incident record updates itself.

- Task assignment with map, context and contact
- Status steps: accepted, on the way, on site, done
- Photo and note capture as proof of work
- Team availability and workload view
- Offline capture that syncs when connectivity returns

WHAT TEAMS GAIN

- Live visibility of field work
- Less phone traffic
- Verified closure of every job

METRICS TO TRACK

- Time to accept a task
- Time to arrive on site
- Share of jobs closed with photo proof
- Reopened jobs

PRACTICAL TIP

Be open with field teams about any location tracking: what is tracked, when and why. Trust drives adoption.

USE CASE 06 OF 10

Emergency and multi-agency coordination

Run a flood, fire or major event from one shared room.

THE CHALLENGE

Major events need police, fire, health, traffic and utilities to work together. Information moves slowly, and no single record shows who decided what.

HOW IT WORKS

A crisis mode opens a shared event room: a common map, a task board for each agency, a decision log and notification lists. SOPs for each type of emergency load as checklists. After the event, the log supports a proper review.

- Event rooms with a shared map and task board
- Pre-loaded SOP checklists for each emergency type
- Mass notification lists and message templates
- Resource tracking for teams, vehicles, pumps and shelters
- A decision log and after-action report

WHAT TEAMS GAIN

- Faster, better-coordinated response
- Every agency works from the same facts
- Learning from every event

METRICS TO TRACK

- Time to open an event room
- Time to notify all agencies
- Share of SOP steps completed
- Joint drills held and reviewed per year

PRACTICAL TIP

Run joint drills with every agency at least twice a year, and update the SOPs with what you learn.

USE CASE 07 OF 10

Traffic and mobility command

Detect blockages and risky locations early, and coordinate the fix.

THE CHALLENGE

Signals, junction cameras, parking and public transport run as separate systems. Congestion and crashes are noticed late.

HOW IT WORKS

The ICCC links signal controllers, junction cameras, parking and transit tracking. Congestion, stopped vehicles and violations appear as events, and operators coordinate with traffic police on the ground and adjust plans.

- Junction and corridor camera integration
- Congestion and stopped-vehicle alerts
- Signal plan status, with overrides only as policy allows
- Parking and transit data on the city map
- Diversion plans for festivals and emergencies

WHAT TEAMS GAIN

- Faster clearing of blockages
- Better coordination of traffic police and city teams
- Data for road engineering

METRICS TO TRACK

- Time to detect a blockage
- Time to clear it
- Violations detected per location
- Average corridor travel time

PRACTICAL TIP

Agree in advance who may change signal plans from the command center, and under what conditions.

Utility and environment monitoring

Find faults before citizens do, and share the alert with every team that must act.

THE CHALLENGE

Water, lighting and environmental data stay inside their own departments. Failures often reach citizens before they reach a control room.

HOW IT WORKS

Sensors and utility systems report to the ICC: water level, flow and pressure, lamp status, air quality, noise and rainfall. Threshold alerts become incidents with owners, and one alert can reach several teams at once.

- Water flow, pressure, level and quality
- Street lighting status and fault reports
- Air quality and noise hotspots
- Rainfall and flood-level alerts
- Maintenance tickets created from faults

WHAT TEAMS GAIN

- Faults found before complaints arrive
- Cross-department response to one alert
- Evidence for planning and maintenance

METRICS TO TRACK

- Share of sensors online
- Time to detect a fault or breach
- Time to repair
- Complaints per asset type

PRACTICAL TIP

Start with assets where failure hurts most, such as flood points, main pumps and arterial lighting, and calibrate sensors regularly.

USE CASE 09 OF 10

Citizen engagement and helpdesk

Connect what citizens report with what the city detects.

THE CHALLENGE

Complaints arrive by phone, app, web and social media. Citizens do not know the status, and each department sees only its own share.

HOW IT WORKS

Helpdesk channels feed the ICCC. Requests are classified, routed to the right team and tracked to closure. Citizens receive updates, and managers see backlog, repeat locations and resolution times next to operational data.

- Multi-channel intake in one system
- Automatic classification and routing
- Status updates to citizens
- Many complaints linked to one incident
- Backlog and repeat-issue dashboards

WHAT TEAMS GAIN

- Faster fixes
- Clear accountability
- Citizens can see results

METRICS TO TRACK

- Time to first response
- Time to close
- Reopen rate
- Citizen satisfaction

PRACTICAL TIP

Publish target resolution times and report against them. Visible commitments build trust.

USE CASE 10 OF 10

Analytics, reporting and digital twin

Use the data the center collects to plan, not just to react.

THE CHALLENGE

ICCCs collect large amounts of data, but few cities use it for planning. Reports are built by hand and arrive late.

HOW IT WORKS

Events, incidents, sensor readings and service data are stored on one data platform. Dashboards and scheduled reports show trends, hotspots and performance. A digital twin lets planners test what-if scenarios, such as closures, heavy rain or large events, before they happen.

- Historical data on incidents and response times
- Hotspot and trend analysis
- Scheduled reports for departments and leadership
- Digital twin scenarios for planning
- Open data views for the public

WHAT TEAMS GAIN

- Decisions based on evidence
- Resources placed where they are needed
- Plans tested before they are needed

METRICS TO TRACK

- Reports delivered on schedule
- Decisions linked to data
- Recurring hotspots reduced
- Scenarios run per quarter

PRACTICAL TIP

List the five questions leaders ask every month and build the reports that answer them first.

03

PART THREE

Making it real

AI agents, people and procedures, security and privacy, a phased roadmap, governance, measures and a readiness checklist.



PART THREE | CHAPTER 5

AI agents in the command center

Software agents that watch live data, understand context and help teams act.

An AI agent is software that observes a stream of data, decides what matters within rules set by people, and then recommends or takes an action. Because agents never tire, they extend the attention of a control room across thousands of cameras, sensors and tickets. Each agent focuses on one job, and all can report to the same command center.

#	Agent	Area	What it does in the command center
1	Incident Response	Public Safety	Ranks alerts, merges duplicates, suggests the team to assign and tracks closure.
2	Video Analytics	Public Safety	Detects and counts people, vehicles and events on camera, and raises clips as alerts.
3	Crowd Management	Public Safety	Estimates crowd density by zone and warns before thresholds are crossed.
4	Traffic Signal	Mobility	Suggests or adjusts signal timing as congestion builds.
5	Road Safety	Mobility	Spots dangerous driving and ranks risky locations.
6	Fire and Safety	Energy and Buildings	Combines fire, heat and access data to confirm events faster.
7	Leak Detection	Water	Flags likely leaks by comparing flow and pressure.
8	Street Lighting	Environment and Streets	Finds faulty lamps and opens work orders.
9	Citizen Helpdesk	Operations and Planning	Classifies complaints, routes them and follows up until closed.
10	Digital Twin	Operations and Planning	Runs what-if scenarios for closures, rain and large events.

AJEEVI offers twenty agents across mobility, water, energy and buildings, public safety, environment and operations. The ten above are the most relevant to a command center.

FOUR LEVELS OF AUTONOMY

- **Observe.** The agent summarizes and alerts. It takes no action.
- **Recommend.** The agent suggests an action and an operator decides.
- **Act with approval.** The agent prepares the action and a person confirms it.
- **Act automatically.** Only for low-risk steps agreed in advance. Most cities should begin at the first two levels.

DESIGN RULES FOR CITY AGENTS

- **People stay in control.** Start with recommendations and allow automatic actions only where agreed in advance.
- **Explain every alert.** Show the data behind each alert, so operators can trust or challenge it.
- **Limit permissions.** Each agent reads and does only what its job needs.
- **Log everything.** Keep a record of what each agent saw, decided and did.

PART THREE | CHAPTER 6

People, SOPs and the operating model

A command center runs on trained people following clear procedures. Technology only supports them.

Role	Responsibility
Operator	Watches screens and alerts, creates and updates incidents, and follows SOPs.
Shift supervisor	Owns the shift, handles escalations, approves actions and runs the handover.
Department liaison	Represents police, traffic, water, power or civic teams on the floor or on call.
Analyst	Tunes rules, builds reports and studies hotspots and response times.
Technical engineer	Keeps the platform, cameras, sensors and networks healthy.
ICCC head	Sets priorities, reports to leadership and owns continuous improvement.

A GOOD SOP FITS ON ONE PAGE AND ANSWERS SIX QUESTIONS

- **Trigger.** What event or alert starts it?
- **Owner.** Who is responsible, and who is the backup?
- **Steps.** What happens, in order?
- **Escalation.** Who is told, and after how long without action?
- **Closure.** What proves the incident is done?
- **Review.** When was it last tested, and when is it next due?

SHIFT HANDOVER

- Hand over open incidents, pending escalations, device outages, planned events and anything unusual, in writing and in person.
- Record the handover in the platform so the next team can see it, and so it can be reviewed later.

TRAINING THAT STICKS

- **Induction** on the platform, the SOPs and the departments the center serves.
- **Scenario drills** using realistic alerts, run on the live system or a safe copy.
- **Refreshers** whenever systems, SOPs or alert rules change.
- **Cross-training** so that leave and turnover do not leave a gap.

PLAN FOR 24x7

Staff the center for round-the-clock coverage, including leave, breaks and training time. Gaps usually appear on the quietest shifts.

PART THREE | CHAPTER 7

Security, privacy and trust

An ICCC holds the most sensitive data a city has. Citizens will accept it only if it is secure and respects privacy.

A command center connects cameras, sensors and systems that were once separate. That makes it powerful, and it also makes it a target. Security and privacy are not add-ons. They shape the design, the contracts and the daily operation.

SECURITY PRACTICES

- **Secure by design.** Encrypt data in transit and at rest, change default passwords, and keep devices and software patched.
- **Network separation.** Keep operational networks apart from public and office networks, and control every connection between them.
- **Role-based access.** Give each person only the access their job needs, and review access regularly.
- **Audit trails.** Record who viewed, exported or changed what and when, especially for video and personal data.
- **Evidence handling.** Require approval for video exports and keep a record of who received them.
- **Standards and testing.** Align with recognized practice such as ISO/IEC 27001 and guidance from CERT-In, and test systems regularly.
- **Plan for incidents.** Have a cyber incident response plan, and rehearse it.

PRIVACY AND ETHICS

- **Purpose limitation.** Collect data only for stated purposes, and tell the public what they are.
- **Retention rules.** Keep data only as long as needed, then delete it.
- **Minimize personal data.** Prefer analytics that count and detect events over analytics that identify people, unless the law and the use case clearly require it.
- **Follow the law.** Comply with applicable laws, including the Digital Personal Data Protection Act, 2023 in India, and seek legal advice for sensitive uses.
- **Human oversight.** A person reviews decisions that affect individuals.
- **Transparency.** Publish policies, and offer a way for citizens to ask questions and raise concerns.

WHY IT MATTERS

Trust is built slowly and lost quickly. Publish your data and privacy policy before the first camera goes live.

PART THREE | CHAPTER 8

A phased roadmap

Start with a focused foundation, expand with confidence, then optimize.

PHASE 1 Foundation	PHASE 2 Expand	PHASE 3 Optimize
Typical timing: first 6 months • Pick two or three high-value capabilities, such as video management, incident management and the city map. • Build the command floor, core platform, networks and data platform. • Integrate existing cameras and the first two or three departments. • Write SOPs, train operators and agree service levels.	Typical timing: 6 to 18 months • Add departments and capabilities that reuse the same platform: traffic, water, buildings, environment. • Roll out mobile apps for field teams and the citizen helpdesk. • Open event rooms for multi-agency coordination and run joint drills. • Add the backup site and introduce AI agents, starting with recommendations.	Typical timing: 18 months onward • Run digital twin scenarios for planning and emergencies. • Use predictive maintenance to fix assets before they fail. • Share data with partner agencies under clear rules. • Review results, retire what does not work and invest where value is clear.

Timings are illustrative. Adjust them to your city, funding and readiness.

MILESTONES TO REVIEW AT EACH PHASE

- The capabilities are live, used daily and trusted by the people who rely on them.
- Measures from Chapter 10 show improvement against the starting point.
- Security, privacy, SOPs and operations are documented and tested.
- Budget, staff and support contracts are in place for the next phase.

ALREADY HAVE AN ICCC?

Start with an honest health check. Which integrations are live and healthy? Which alerts are acted on? Which SOPs are used? Fix those gaps before adding anything new.

ADVICE FROM THE FIELD

Pilot first. A small, well-run deployment that people trust is the best argument for the next phase.

PART THREE | CHAPTER 9

Governance, procurement and operations

Good technology fails without clear ownership, sound contracts and trained operators.

Role	Responsibility
City leadership and steering committee	Sets goals, approves budgets and policies, and sponsors cooperation between departments.
ICCC head and team	Runs the center around the clock, manages alerts, coordinates response and reports results.
Departments	Own their use cases, provide field teams, keep SOPs current and act on tasks from the center.
IT and security	Run infrastructure, manage access, protect data and handle cyber incidents.
Partner and AMC provider	Deliver, support and maintain systems under agreed service levels.

PROCUREMENT CHECKLIST

- **Outcomes first.** Write requirements around results and measures, not only equipment lists.
- **Open interfaces.** Require documented APIs and standard protocols.
- **Named integrations.** List the systems to be connected, with protocols, owners and test scenarios.
- **Data ownership and exit.** Confirm the city owns its data and can export it in usable formats.
- **Service levels.** Define uptime, response and repair times for a 24x7 center, and link payment to them.
- **Local support.** Check for trained engineers, spares and response times near your city.
- **Cybersecurity.** Ask for security testing, patching commitments and incident reporting.
- **Scalability.** Confirm the platform can add departments and use cases without rebuilding.
- **Acceptance by scenario.** Accept the system by running real SOP scenarios end to end, not only by checking equipment.
- **Total cost.** Compare multi-year costs including maintenance, connectivity and training.

OPERATIONS THAT KEEP THE CENTER HEALTHY

- Plan annual maintenance contracts (AMC) and spares from the start.
- Monitor the health of cameras, sensors, networks and integrations, and fix faults quickly.
- Use change control for rules, SOPs and integrations, so updates are tested and recorded.
- Train operators, refresh the training when systems change, and review incidents regularly.

PART THREE | CHAPTER 10

Measuring success

What gets measured gets improved. Choose a few measures in each area and track them from day one.

Area	Example measures
Detection	Time to detect an event; share of events found by the system rather than reported by citizens
Response	Time to acknowledge, assign, arrive on site; share of incidents closed within target
Alert quality	False alert rate; alerts per operator per hour; share of alerts acted on
Coordination	Time to notify all agencies; share of SOP steps completed; joint drills held
Platform health	Cameras and sensors online; integrations live; system uptime; data quality
Adoption	Active users per week; departments connected; incidents handled on the platform, not by phone
Citizen outcomes	Time to first response and to close; reopen rate; satisfaction; repeat problems by area
Resilience	Failover test results; recovery time achieved; time to restore a failed site

HOW TO USE THESE MEASURES

- **Record a baseline.** Measure how things work today, before launch, so improvement is visible.
- **Set targets with the departments involved.** Shared targets create shared ownership.
- **Review monthly.** Show results on the command center dashboard and discuss what to change.
- **Report to citizens.** Publish a short summary of outcomes, so the public can see the benefit.
- **Watch the whole system.** Track platform health and adoption alongside outcomes.

KEEP IT SIMPLE

Choose fewer measures and track them well. A short list that people trust beats a long list nobody reads.

PART THREE | CHAPTER 11

Common pitfalls and a readiness checklist

Most problems in command center programs are about people and process, not technology.

Pitfall	How to avoid it
A video wall without workflows	Build incident management, SOPs and escalation first, then the screens.
Buying technology before defining the problem	Start from outcomes and measures, then choose tools.
Separate systems with separate screens	Integrate through one platform and open interfaces.
No operating procedures	Write SOPs and train operators before go-live.
Too many alerts	Tune rules on a few locations first and add more gradually.
Departments that do not take part	Give each department an owner, a liaison and shared targets.
Neglecting maintenance	Budget for AMC, spares and monitoring from day one.
Weak data quality	Calibrate sensors, check for gaps and flag bad readings.
Privacy as an afterthought	Publish policies, minimize personal data and limit access.
Vendor lock-in	Require open APIs, data ownership and exit terms.
No backup plan	Build a DR site and rehearse failover.

READINESS CHECKLIST

Question	Yes / No
Do we have two or three clear problems to solve first?	[]
Does each have an owner and agreed measures?	[]
Do we know which systems and data already exist, and how they connect?	[]
Have we decided where data will live and who can see it?	[]
Are SOPs, staff, shifts and training planned?	[]
Is there a backup site or plan for when the center fails?	[]
Is funding secured for operations, maintenance and AMC?	[]
Have we set a privacy and security policy?	[]

REFERENCE

Glossary

Plain-language definitions of the terms used in this ebook.

Term	Meaning
AI agent	Software that watches data, decides within rules and recommends or takes action.
AMC	Annual maintenance contract for support and repair of installed systems.
API	Application programming interface. A documented way for systems to exchange data.
BMS	Building management system that controls HVAC, lighting, access and safety.
CAD	Computer-aided dispatch. Software that records emergency calls and assigns responders.
Digital twin	A live digital model of a city or asset, used to monitor and test scenarios.
DR	Disaster recovery. A backup site and plan that keep systems running if the main site fails.
Edge	Computing done close to the camera or sensor instead of in a distant data center.
GIS	Geographic information system. Software that works with maps and location data.
ICCC	Integrated command and control center that brings city systems onto one platform and one floor.
IoT	Internet of Things. Connected devices and sensors that send data.
ITS	Intelligent transport systems for managing traffic and road safety.
MQTT	A lightweight messaging protocol commonly used by IoT devices.
ONVIF	An open standard that lets cameras and video software from different makers work together.
PTZ camera	A camera that can pan, tilt and zoom.
RTO / RPO	Recovery time objective and recovery point objective: how long a system may be down and how much data may be lost.
SCADA	Systems that monitor and control utility and industrial equipment.
SLA	Service level agreement. Agreed targets for uptime, response and repair.
SOP	Standard operating procedure. Written steps for how a task or incident is handled.
Sovereign AI	AI whose models and data are hosted and controlled within a country or organization.
VMS	Video management system. Software that records, stores and manages camera streams.



ABOUT AJEEVI

HumanTech for a smarter world

AJEEVI Technologies builds AI, IoT and software for smarter urban infrastructure. Made in India. Built for the world.

Our platforms help cities, utilities, campuses and industries watch, detect and respond across traffic, water, energy, buildings and public safety.

PLATFORMS

GyanAkshi	AI and video analytics
GyanYantram	IoT devices and sensors
GyanKendram	Integrated command center
GyanBhawan	Smart buildings and BMS
JalAJV	Water intelligence
VayuAJV	Environmental intelligence
TransAJV	Smart mobility
GyanSatark	Public safety
GyanRakshak	Citizen and operations helpdesk

TALK TO US ABOUT YOUR CITY

Website: www.ajeevi.com

Email: hello@ajeevi.in