Halo®

Taxonomies of Control Rooms

Next Generation Control to Safeguard the Public Efficiently

Executive Summary

As risk landscapes grow more complex, public venues & events must rethink how safety, security, and accountability are delivered. From terrorism threats and cyberattacks to staffing shortages and rising operational costs, traditional incident control methods can no longer keep pace. At the centre of all risk management sits the control room; the nerve centre of public safety.

This white paper presents a new framework for understanding and modernising control rooms. It outlines five stages of control room evolution, identifies common pitfalls, and explains how Halo's Next Generation Incident Management System (IMS) empowers organisations to improve safety, compliance, and operational efficiency, while reducing costs.

1 Introduction: The Evolving Risk Landscape

Public safety concerns increasingly dominate the agenda for all event organisers. The introduction of The Terrorism (Protection of Premises) Act 2025 – also known as Martyn's Law – has focused attention on accountability and the risks associated with terrorism. But organisers are also managing a complex and diverse range of other risks, from the traditional health and safety challenges and staffing shortages, to rising costs, an escalation in cyber attacks, and everything in between.

The beating heart of all public venues, and the focal point of converging risks and how they are mitigated, is the control room. So it stands to reason that every control room should have a single 'black box' for capturing real-time information, actions, and evidence that supports businesses, staff and the public they are protecting.

This white paper explores 'Control rooms' and their technological categorisations in an informal, jargon free way, so that we can all start to understand the environments in which we're operating and have a clear direction of travel to deliver continuous improvement and protect everyone.

This is especially important, given the increasing challenges associated with recruiting and affording the staff required to provide security, maintenance, cleaning and medical services following the increase in national insurance and minimum wage, and the lack of available and suitably trained people, mean these three things, complex threat landscapes, high staff cost and lack of staff resource converge to make the perfect storm for control rooms.

When confronted with competing threats, reduced budgets, and limited resources, how can businesses improve the effectiveness of their operating models? What is the best way to achieve accountability while relying on multiple contractors to deliver core services? . And, critically, how does the overall experience affect both customer perception of safety and their enjoyment, empowering repeat business and growth?

2 The Case for Control Room Modernisation

The escalating focus on public safety created by the ratification of The Terrorism (Protection of Premises) Act 2025, also known as Martyn's Law has reinforced awareness of safety procedures and the resources required in a continuously evolving threat landscape. While an essential step in creating a consistent, coherent approach to safety, it is important to remember that safeguarding the public is not just about ticking the boxes required by regulation.

Safeguarding the public is a vital aspect of the overall attendee experience and a chance to build credibility and trust with customers. **When people feel safe, they will stay longer on site and, as a result, spend more money.** Most importantly, they will come back: dwell time and repeat business have long been seen as key metrics that directly impact bottom line.

The challenge for public venues & events is how best to achieve accountability and reinforce public safety within existing financial constraints, especially when so many services are delivered by third parties and prices are rising. What is the best approach to ensure accurate information collection, incident sharing and resource management plotted against risk and effective cross-department collaboration?

There is no doubt that technology has provided a platform to transform the speed of response and depth of understanding in recent years. In an era of ubiquitous mobile communication and cloud data storage, there are still some businesses that are 100% reliant on the analogue-generation approach to incident management, using pen and paper to record incidents.

However, the majority are now exploring how to use digital systems and are seeking information on how to transition their control rooms and businesses through the tiers, from analogue (pen & paper) or digital (spreadsheets or word docs) through second or third generation transformations. It is largely recognised that these legacy systems have significant gaps and would be exponentially improved in both effectiveness and safety.

Adding a second-generation use of WhatsApp messaging to word documents and spreadsheets, for example, still requires dedicated control centre staff to transcribe incident information, slowing response and adding cost, while not delivering any significant improvement to the evidential standard of the control room, the integrity and trustworthiness of its audit trail, or any efficiencies brought about by trend analysis or resource to risk mapping.

3 Scope & Definitions: Re-Defining Control Room Maturity

There exists a wealth of control room classifications. It's fair to say, the landscape is very broad, with almost no universal consensus from one industry to another as each has their own technological needs, acronyms and standards at the local level. So for clarity, these have been separated into three distinct areas:

1. International, cross industry standards
2. Sector or region-specific rules/regulations
3. De-facto industry taxonomies promoted by vendors and integrators

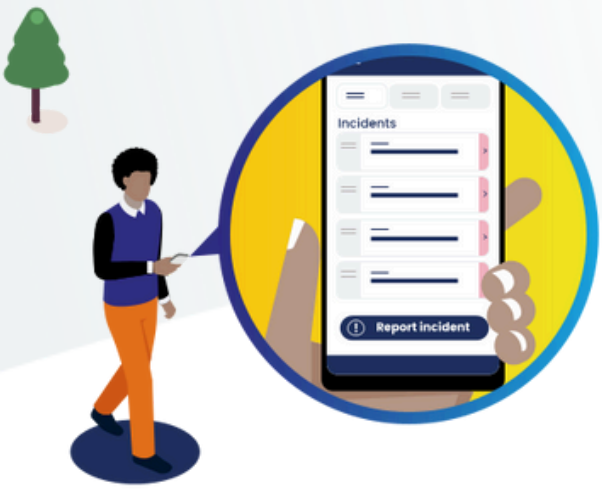
Across the industries we serve, control room standards and classifications vary significantly. International standards such as ISO 11064, IEC frameworks, and EEMUA guidance play an essential role in shaping physical control room design, particularly around ergonomics, layout, and infrastructure. These standards are definitive, not interpretative – they either apply or they don't, and they remain critical for those operating at a strategic or facilities level.

However, for the purpose of this white paper, the focus is operational rather than architectural. While permanent vs. temporary and staffed vs. unstaffed control rooms are important distinctions, these are best addressed through the detailed documents and specifications developed by the standards bodies themselves.

Similarly, sector-specific regulations, ranging from power transmission and alarm receiving centres to media broadcast hubs and the health sector, are essential for those environments. But compliance with those regulations is binary: organisations either meet the required standard or they do not. As a result, debating their nuances lies outside the scope of this paper.

Halo Solutions works across all of these regulated sectors, ensuring our technology aligns with current compliance obligations. Our approach is to follow global standards and regulations where necessary, while also asking critical questions that drive innovation in the operational reality of control rooms.

This paper therefore focuses exclusively on control room taxonomy from a functional and technological standpoint. It presents a clear, five-stage model of evolution – spanning Analogue > Digital > Web-Based > Next Generation > Future Generation – to help security leaders assess their current maturity and define a roadmap for transformation.



4 Control Room Maturity: Five Tiers of Evolution

Just as aircraft rely on black boxes for accountability and insight, control rooms must serve the same purpose for safety operations; recording what was known, when, by whom, and what actions were taken. In today's regulatory and risk environment, particularly under Martyn's Law, the absence of a robust digital Incident Management System (IMS) leaves organisations exposed. A modern control room must act as a trustworthy source of truth; protecting people, reputations, and decision-makers alike.

Tier 1: Analogue Systems – Pen and Paper Logging

Control rooms operating at this level rely on handwritten records and radio communication. While this setup may include CCTV and other tech inputs, the core incident recording remains fully manual.

Advantages:

- Low cost, easy to implement
- Familiar and intuitive to most operators
- No reliance on power, internet, or devices

Disadvantages:

- Handwriting can be illegible or altered
- Logs are not time-stamped or verifiable
- Offers no data for trend analysis or future planning
- Impossible to prove contemporaneity or chain of evidence

In practice, these systems deliver little to no medium- or long-term value. Although the upfront cost is minimal, the downstream risks and inefficiencies are significant. You cannot analyse what you don't accurately record.

Tier 2: Digital Standalone Systems – Word and Spreadsheet Logging

A step above pen and paper, this tier introduces basic digital tools, typically Word documents or spreadsheets used within the control room.

Advantages:

- Improved legibility and basic organisation
- Low cost and easy to customise
- Better than handwritten records in court or audits

Disadvantages:

- Still reliant on manual transcription and human memory
- Logs can be altered without trace
- Operators often fall back to handwritten notes during peak times
- No integrated workflow or data automation

Critically, these systems cannot guarantee the integrity of records. While file timestamps and metadata offer limited reassurance, they do not provide forensic-level verification. These platforms are not scalable, lack incident lifecycle tracking, and fail to support multi-agency collaboration.

4 Control Room Maturity: Five Tiers of Evolution

Tier 3: Web-Based Systems – Basic Digital Collaboration

Web-based IMS platforms allow for real-time access by remote users and begin to centralise reporting and communication.

Advantages:

- Accessible from multiple locations
- Potential for role-based access and permissions
- Digital logs that are harder to alter post-event

Disadvantages:

- Still requires manual data entry and triage
- Often adapted from generic collaboration tools like Teams or Slack
- Limited scalability and feature growth
- Cannot automate or intelligently triage incidents

These systems often suffer from feature stagnation or "technical debt." While they present as modern solutions, their limitations become evident under operational pressure or during complex, multi-agency incidents.

Tier 4: Next Generation Control Rooms – Mobile-Enabled Incident Management

This tier marks a transformational step. A Tier 4 system includes mobile app functionality, allowing direct input from frontline staff and, ideally, the public.

Key Features:

- Mobile app for reporting and logging
- Integration of images, video, GPS, and real-time updates
- Reduction in radio traffic and operator load
- Structured incident lifecycles and triage workflows
- Public-facing reporting via QR code, SMS, or URL

Operational Benefits:

- Increased collaboration across departments and agencies
- Faster and more reliable evidence capture
- Resource-to-risk mapping and trend analysis
- Enhanced public confidence and safety perception

Fourth generation systems shift control room operators from reactive loggists to orchestrators of information. The platform absorbs much of the administrative burden, enabling faster response and smarter resource deployment. With structured workflows, digital SOPs, and audit-ready logs, Tier 4 IMS platforms are aligned with both operational excellence and regulatory compliance.

5 Tier 5: The Future of Control Rooms – Integrated AI & Automation

The future of control room technology lies in intelligent integration. A Tier 5 system doesn't just record, it thinks, reacts, and orchestrates a network of smart technologies.

Examples of AI-Driven Automation:

- A fire alarm triggers camera focus, incident creation, and responder alerting
- Computer vision detects aggression or crowding and flags it for operator review
- A fatality incident triggers automated alerts and schedules a multi-agency response call

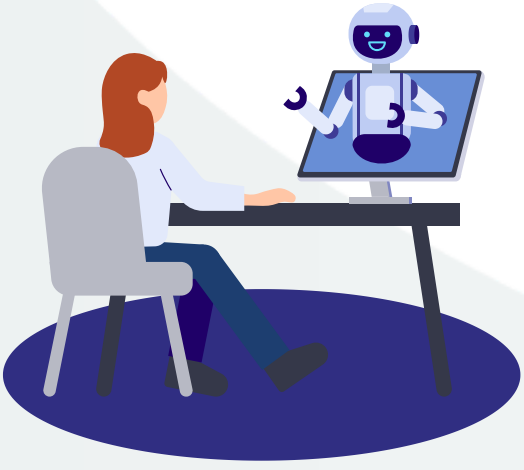
Key Characteristics:

- Multi-system integration (CCTV, comms, fire, access control)
- AI-generated insights and decision support
- Human-in-the-loop design to safeguard automation integrity

While the promise of Tier 5 is powerful, the market is still maturing. Halo's approach is to observe this space with caution, focusing first on delivering the most secure, cost-effective, and operationally valuable Tier 4 system available today.

By framing the control room as the black box of public safety, we can shift the narrative from compliance and admin to trust, accountability, and continuous improvement. With Martyn's Law coming into force and the risk landscape evolving rapidly, organisations must assess their control room maturity and act accordingly.

Halo Solution's Tier 4 IMS is already enabling organisations to meet these challenges head-on, empowering teams to work smarter, safer, and with full transparency.



6 The Halo System: Tier 4 Control Made Easy

Halo is a Tier 4, Next Generation Incident Management System (IMS), purpose-built to directly address and resolve the critical operational failures identified in major incidents such as Hillsborough, Manchester Arena, and Astroworld. It has been designed from the ground up to embed and automate the essential processes required to protect organisations, their teams, and the public. This mission is reflected in Halo's core ethos: "Let's protect everyone."

Within the global marketplace, only a small number of IMS platforms meet the criteria to be classified as Tier 4. While each offers its own configuration of features and modules, Halo distinguishes itself through its balance of advanced capability, operational simplicity, and cost-effectiveness.

Tier 5 systems, those offering advanced AI integration and automated multi-system orchestration, are even rarer, particularly within the private sector. However, their high cost places them well beyond the reach of most organisations. As a result, Tier 4 represents the current sweet spot for innovation, capability, and scalability.

It is important to note that these tiers are not rigid but evolutionary. While it is not possible for an analogue (pen and paper) system to evolve directly into a digital spreadsheet solution, it is possible for a Tier 3, web-based system to develop a dedicated mobile app and elevate itself into Tier 4. Likewise, a Tier 4 system can ascend to Tier 5 by building or integrating with AI-powered technologies, provided it does so thoughtfully and securely.

That said, cost remains a central consideration. Tier 3 platforms may offer lower initial price points, while Tier 4 systems can often deliver significantly greater long-term value. As systems mature, maintaining relevance and usability becomes as important as adding new features.

At Halo, our focus is clear: we aim to build the most comprehensive, intuitive, and cost-effective Tier 4 IMS on the market. While we recognise the growing interest in AI, we are approaching this space with deliberate caution. Many platforms are not developing proprietary AI but are instead integrating third-party technologies, raising important questions around data sovereignty, privacy, and security.

These issues are not yet fully resolved, and we believe our clients deserve a higher standard of assurance before AI is deployed within core safety systems. Additionally, current AI-generated incident summaries and recommendations often lack the nuance and domain-specific understanding required in complex environments. As such, Halo is choosing to watch, learn, and prepare, rather than rush. Like Apple, we believe in getting it right, not simply getting there first.

7 The Strategic Value of Modern Incident Management

Operational safety and security are under more pressure than ever before. Across sectors, the question practitioners face daily is: **how can we achieve more with less?** This is where Halo provides immediate, practical value—helping organisations streamline operations while enhancing accountability and responsiveness.

In the UK, the next 18 months will see the Security Industry Authority (SIA) release further guidance on the implementation of Martyn's Law, prompting organisations to review their current procedures, policies, and resource allocations. Many will begin identifying gaps and assessing how to meet new statutory requirements, while continuing to manage existing risks and responsibilities.

Yet, it's essential not to become overly focused on new regulations alone. The so-called "old risks" are not disappearing. As demonstrated by the recent cyberattack on Marks & Spencer, threats continue to evolve, and vulnerabilities exist across every industry. This reinforces a core truth: the effectiveness with which an organisation manages incidents impacts not just compliance, but its financial performance and customer confidence.

Universities that appear unsafe lose student applications. Overcrowded, insecure transport hubs deter commuters. Eventgoers who feel unsafe spend less time—and less money—on site, and are less likely to return. By contrast, environments that are perceived as safe see increased dwell time, repeat visits, and higher levels of satisfaction and revenue.

This is the foundation of public safety economics, the link between perceived safety and commercial success. Increasingly, this includes scrutiny of how well safety and security operations are managed, documented, and evidenced.

Organisations that perform best in this space have something in common: a reliable, data-rich Incident Management System (IMS). These systems serve as the "black box" for the business, capturing, organising, and surfacing insights that inform data-driven, evidence-based decision making.

Ultimately, the right IMS doesn't just help you meet compliance requirements. It helps you **save time, money, and lives.**

Find out how Halo can help you save time, money and lives

Halo®