

A Guide to Making Confident Control Room Technology Decisions

Make High-Stakes Decisions with Certainty.



Introduction

Control room technology should amplify operational capability, not create it. Yet many organisations discover that impressive platforms deliver disappointing results. The root cause is rarely the technology itself. It is investing in systems before the operational foundations are ready to support them.

This guide helps Directors of Security, COOs, and executive leaders understand what needs to be in place before engaging technology suppliers. It addresses the questions that should be answered internally before procurement begins, and provides a framework for evaluating suppliers once operational readiness has been confirmed.

Technology procurement is not the starting point for control room transformation. It is the accelerator applied once the foundations are in place.

Maturity Before Modernisation

New technology does not fix structural problems. It makes them faster, louder, and more expensive. A control room with unclear escalation protocols will not gain clarity from better dashboards. Operators who struggle to make decisions under pressure will not become confident because alerts arrive more quickly.

Modernisation accelerates whatever operational reality already exists. If that reality is fragmented, investment just creates sophisticated chaos.

What Technology Cannot Fix

No platform can compensate for:

- Undefined decision authority frameworks
- Unclear strategic intent
- Inconsistent processes
- Capability gaps in leadership
- Cultural behaviour that suppresses early warnings

These are structural issues that technology will magnify, not resolve. Investment in systems before addressing these foundations creates expensive disappointment.



The 7 Pillar Technology Readiness Assessment

Control room maturity is the alignment of strategy, people, and systems to enable consistent decision-making under pressure. The 7 Pillar Control Room Framework™ provides the lens through which operational readiness should be assessed before technology investment.

Before engaging technology suppliers, executive leaders should understand how their operation performs across all seven pillars:

Pillar 1: Strategy

Key Question: Is strategic intent explicit, or has it evolved by default?

Technology must serve a clear strategic purpose. Without explicit intent, procurement becomes reactive and driven by suppliers rather than operational needs. Before evaluating systems, leaders should confirm that strategic direction is documented, understood, and aligned with organisational risk appetite.

Pillar 2: People

Key Question: Does technology reduce cognitive load and fatigue, or increase it?

Control room operators work under sustained attention demands. Technology should filter noise, prioritise signals, and reduce mental burden. Systems that increase information volume without improving clarity create cognitive overload and accelerate fatigue. Before procurement, organisations should assess whether new platforms will genuinely reduce operator workload or simply add complexity to existing strain.

Pillar 3: Culture

Key Question: Does culture support early warnings and learning, or suppress uncertainty?

Technology that surfaces risk signals is valuable only if culture permits those signals to be acted upon. Platforms that increase visibility are wasted when psychological safety is absent and early warnings remain ignored.

Pillar 4: Environment

Key Question: Does technology support operator wellbeing and operational collaboration?

Control room technology should enhance both individual operator wellbeing and team collaboration. Systems that create isolated working patterns or inhibit communication between operators reduce operational effectiveness. Technology procurement should evaluate how platforms enable coordination, information sharing, and peer support during high-tempo operations, whilst also considering ergonomic interfaces that reduce physical and mental strain during extended shifts.

Pillar 5: Operations

Key Question: Does technology support SOP workflow, decision-making, and escalation processes?

Control room technology should align with established Standard Operating Procedures whilst supporting operators when procedures prove insufficient. Systems should guide workflow during routine operations, provide decision support when complexity increases, and enable clear escalation pathways when situations exceed defined parameters. Before procurement, organisations should evaluate whether platforms will integrate with existing SOPs or require fundamental operational redesign, and whether technology genuinely supports adaptive decision-making or simply automates rigid processes.

Pillar 6: Technology

Key Question: Do current systems support or obstruct decision-making?

Before procuring new platforms, organisations should assess whether existing systems are being used effectively. Unused functionality often signals process problems rather than capability gaps. Procurement becomes clearer when current limitations are precisely understood.



Pillar 7: Data

Key Question: Does technology build situational awareness, support decision-making, and use analytics to reduce cognitive load?

Effective control room technology transforms raw data into actionable intelligence. Systems should present information that builds situational awareness rapidly, highlight decision-relevant signals, and use analytics to filter noise rather than amplify it. Before investing in data platforms, organisations should assess whether technology will create meaningful intelligence that reduces operator burden, or simply generate more dashboards that operators must interpret under pressure.

Key Questions Before Technology Selection

Once operational foundations have been assessed, these questions help executive leaders define requirements clearly before engaging suppliers:

Strategic Clarity

- What specific operational outcomes must technology enable?
- How does this investment align with documented strategic intent?
- What would operational success look like 12 months after implementation?

Cognitive Load and Operator Performance

- Will new systems reduce information overload or increase it?
- How will technology filter noise and prioritise decision-relevant signals?
- What evidence exists that proposed systems reduce operator fatigue rather than compound it?

Operator Wellbeing and Collaboration

- Does technology enable effective team coordination and information sharing?
- How do interfaces support operators during extended shifts without increasing physical or mental strain?
- Will systems enhance peer support and collaborative problem-solving during incidents?

Integration and Compatibility

- What existing systems must integrate with new platforms?
- What data must flow between systems, and who defines integration requirements?
- How will integration complexity affect implementation timelines and operational disruption?

Situational Awareness and Decision Support

- How will technology build shared situational awareness across the team?
- What analytics capabilities exist to surface decision-relevant patterns and reduce manual analysis?
- Does the system provide actionable intelligence or simply more data to interpret?

SOP Workflow and Escalation

- How does technology align with existing Standard Operating Procedures?
- Does the platform guide workflow during routine operations whilst supporting adaptive decision-making when complexity increases?
- Are escalation pathways clearly defined and supported by the system when situations exceed standard parameters?

Training and Capability Development

- How intuitive is the system for operators under pressure?
- What training is required, and how realistic is the timeline given operational demands?
- Will technology complement existing capabilities or require fundamental skill development?



Change Management

- How will operational disruption be managed during implementation?
- What governance will oversee implementation and resolve conflicts?
- Who owns accountability when systems fail to deliver expected outcomes?

Risk and Resilience

- What happens if systems fail during critical incidents?
- Are backup procedures documented and tested?
- How will supplier support respond during operational pressure?

Preparing for Supplier Engagement

Once internal readiness has been assessed and requirements have been clarified, effective engagement with technology suppliers requires specific preparation.

Suppliers consistently identify three areas where client clarity accelerates productive conversations and reduces procurement risk:

1. Define Strategic and Operational Outcomes

Suppliers cannot propose effective solutions without understanding what success looks like operationally. Technology procurement should be outcome-led, not feature-led. Before engaging suppliers, executive leaders should document:

- What specific business problem is being solved
- What operational outcomes define success (response times, incident reduction, compliance improvement, risk visibility)
- What measurable results will demonstrate return on investment
- What risks are being reduced or managed (security, safety, operational, reputational)

Without defined outcomes, procurement discussions focus on features rather than capability. This creates expensive solutions that may not address actual operational needs.

2. Document Existing Technology Environment

Suppliers require clear understanding of current infrastructure to propose realistic integration approaches and accurate implementation timelines. Before initial conversations, organisations should compile:

- Current systems in scope (CCTV, access control, PSIM, communications, building management)
- Scale and scope (number of sites, cameras, doors, operators, control room locations)
- What will be retained and what will be replaced
- Infrastructure constraints (network capacity, connectivity, IT policies)
- Integration requirements with existing platforms
- Deployment preferences (on-premises, cloud, hybrid)

Organisations that provide this context receive more accurate proposals and realistic implementation plans. Those that cannot articulate current environment often receive generic solutions that prove incompatible with operational reality.

3. Establish Governance and Stakeholder Alignment

Technology procurement fails when stakeholder alignment is absent. Suppliers need to engage with decision-makers who can commit resources, approve requirements, and resolve conflicts. Before initial engagement, organisations should confirm:

- Who owns the project and who will own the platform operationally
- Executive sponsorship and board-level accountability
- Budget authority and procurement timelines
- Internal stakeholders who must be consulted (security operations, IT, compliance, facilities, finance)
- Decision-making authority and approval processes

Effective supplier engagement typically requires cross-functional input from security or control room leadership, IT and infrastructure teams, compliance and risk functions, procurement or commercial teams, and executive sponsors. Early stakeholder involvement ensures operational, technical, security, and budget considerations are aligned from the outset, reducing risk and preventing costly redesigns during implementation.

Additional Clarity That Accelerates Procurement

Beyond the three core areas above, suppliers also value clarity on:

- End-user roles and workflows (who will use the system daily, how many operators, shift patterns)
- Tolerance for false positives versus missed events (particularly relevant for analytics and alarm management)
- Current maintenance and support arrangements
- Compliance requirements and data governance constraints
- Plans for future expansion or capability development

Organisations that invest time defining these areas before supplier engagement receive more relevant proposals, more accurate costings, and more realistic implementation plans. Those that begin supplier conversations without this clarity often experience scope drift, budget overruns, and delayed timelines as requirements are refined during procurement rather than before it.

Evaluating Suppliers

Once operational readiness is confirmed and requirements are clearly defined, supplier evaluation becomes more objective. These factors separate suppliers who understand mission-critical environments from those who simply sell platforms:

Operational Experience

- Has the supplier delivered for organisations with similar operational complexity?
- Do they understand control room maturity, or only system functionality?
- Can they demonstrate outcomes achieved, not merely systems installed?

Implementation Approach

- Does implementation begin with operational assessment, or technology deployment?
- How do they manage disruption during transition?
- What governance structure do they propose for resolving conflicts during implementation?

Support and Resilience

- What support is available during critical incidents?
- Are response times contractually defined for high-priority failures?
- How do they handle system outages that coincide with operational pressure?

Cultural Fit

- Do they ask questions about operational maturity before proposing solutions?
- Do they demonstrate understanding of human factors and decision-making under stress?
- Are they comfortable challenging assumptions when requirements conflict with best practice?

Commercial Clarity

- Are costs transparent and aligned with realistic implementation timelines?
- What happens when requirements change during implementation?
- How are disputes resolved when performance does not match commitments?

Conclusion

Technology procurement is not where control room transformation begins. It is the accelerator applied once operational foundations are proven. Organisations that invest in understanding their current maturity before engaging suppliers make more confident decisions, achieve better outcomes, and avoid expensive disappointment.

The questions in this guide help executive leaders assess readiness internally before external conversations begin. When procurement is founded on operational clarity rather than reactive pressure, technology delivers the capability improvement and risk reduction that boards expect.

Maturity before modernisation is not caution. It is confidence.

Supplier Profiles

This guide is accompanied by a series of one-page supplier profiles from selected partners within DG Advisory's network. These suppliers have been invited to participate based on their demonstrated experience delivering control room technology in mission-critical environments.

DG Advisory is technology agnostic and operates independently as neither a reseller nor an integrator. Our role is to help clients understand operational readiness before technology investment and to provide frameworks for objective supplier evaluation.

The suppliers featured in these profiles represent different approaches, capabilities, and commercial models. Inclusion does not constitute endorsement. Clients remain responsible for conducting their own due diligence, reference checks, and evaluation processes.

PSIM | Incident Management Systems

Advancis Software & Services

Contact: Richard Dover

Email: richard.dover@advancis.net

Website: www.advancis.net

advancis**WinGuard****Solution**

WinGuard is an open, vendor-neutral Physical Security Information Management (PSIM) platform that integrates multiple systems, such as CCTV, access control, fire, building management, and communication technologies, into a single unified interface for centralised monitoring and control. The platform collects and visualises events from all connected systems in real time, giving operators full situational awareness and enabling faster, more informed decision-making. It supports guided workflows and standard operating procedures, helping users respond to incidents consistently and efficiently. WinGuard is highly scalable and customisable, with hundreds of integration drivers and modular extensions.

Key Capabilities

- System Integration: Connects and unifies multiple security and building systems into one platform
- Centralised Monitoring: Provides a single interface for real-time visibility of all events and alarms
- Workflow Automation: Executes predefined processes and standard operating procedures during incidents
- Alarm Management: Correlates, prioritises, and manages alarms to reduce operator overload
- Reporting and Audit: Logs all events and actions, generating reports for analysis, compliance, and optimisation

Approach

WinGuard enables organisations to move from reactive security operations to a proactive, outcomes-driven model. By unifying data across systems, it reduces operational risk, improves response times, and enhances overall resilience. Its open architecture protects existing technology investments while allowing future scalability and integration. For executive leaders, this translates into lower total cost of ownership, improved compliance and auditability, and better alignment between security, safety, and business operations. It also supports digital transformation initiatives by turning disparate system data into actionable intelligence that can inform strategic decision-making.

Video Wall | Display Management

Aura Vision SL

Contact: Gerardo Grasa

Email: gerardo@auravision.es

Website: www.auravision.es



COMET-C Series

Solution

The COMET-C PRO series is Aura Vision's flagship LED display platform, purpose-built for mission-critical visual environments including command centres, security operations centres, and broadcast studios. Engineered for always-on operational use, it delivers exceptional brightness, image depth, and colour accuracy whilst keeping power consumption and heat output low. With its largest panel in the COMET-C family and advanced Cold LED thermal architecture, the PRO series is designed to perform consistently over long operating hours – making it a compelling choice for control rooms where display quality and reliability are non-negotiable.

Key Capabilities

- Flip-Chip COB technology: Reduces energy waste and improves heat dissipation, supporting long-term colour stability and component longevity.
- Silent, low-heat operation: Cooler running temperatures improve operator comfort and reduce HVAC load.
- 24/7 redundancy: Power and signal redundancy ensure uninterrupted operation around the clock.
- Visual performance: Anti-reflective coating and consistent contrast maintain clarity in high-ambient-light environments.
- Flexible and maintainable: Modular design supports varied deployment configurations and straightforward servicing.

Approach

Aura Vision's engineering philosophy centres on delivering the best possible image whilst reducing power, heat, and long-term operational impact. Rather than prioritising headline specifications, the team focuses on the practical realities of control room use – where displays run continuously, operators work in close proximity for extended periods, and total cost of ownership matters as much as initial performance. Efficient power use helps lower total cost of ownership over the lifetime of the installation, whilst the thermal design reduces dependency on supplementary cooling infrastructure. This approach was recognised with a 2026 Inavation Award for Display Technology – Aura Vision's first industry accolade – affirming the product's real-world relevance for professional and mission-critical environments.

Video Wall & Display Management | Access Control Management | Incident Management Systems | Video Management System | Communications Management

Gallagher Security Europe

Contact: Daniel McKeon

Email: daniel.mckeon@gallagher.com

Website: security.gallagher.com/en-GB



Solution

Gallagher's Command Centre is the powerful software at the heart of Gallagher's integrated security solutions – a centralised platform that gives operators unparalleled control of every aspect of their site, covering people management, access control, site operations, business management, and building systems. Fully scalable from a single door to thousands of access points, Command Centre grows with operational needs, with cloud flexibility enabling secure site management from any location.

Key Capabilities

- Integrated access control: Manages access control, visitor management, credential lifecycle, and emergency response, including biometric and mobile credentials.
- Perimeter and site security: Integrates with ground sensors and perimeter detection for real-time situational awareness and automated alarm responses.
- Third-party integrations: Connects with VMS, intercoms, elevators, HR, building management, and PSIM platforms within a single unified environment.
- Compliance and reporting: Supports regulatory compliance, site health and safety management, and real-time audit reporting.
- Remote and cloud management: Command Centre Web enables secure, MFA-protected site management from any internet-connected device.

Approach

Gallagher takes an integrated platform approach to physical security, consolidating access control, perimeter management, video, building systems, and compliance into a single, fully configurable environment. Powered by Gallagher's proprietary HBUS protocol, the platform ensures fast, secure data exchange across all connected systems. This hardware-level encryption, combined with support for NPSA, CAPSS, and AACS high-security standards, makes Command Centre a credible choice for the most demanding and regulated operational environments. Continuous investment in research and development – evidenced by regular platform releases packed with new integrations and enhancements – reflects Gallagher's commitment to keeping pace with evolving security requirements.

PSIM | Video Management System | Video Analytics | Access Control Management | Communications Management | Incident Management Systems

Genetec Inc.

Contact: Daniel Meyrick
Email: dmeyrick@genetec.com
Website: www.genetec.com



Genetec Security Center

Solution

Genetec Security Center is a unified physical security platform that brings video surveillance, access control, ALPR, communications, intrusion monitoring, and more into a single, intuitive interface. It centralises real-time security data, enabling operators in mission-critical control rooms to monitor events, investigate incidents, and coordinate responses without switching between systems. This unified approach improves situational awareness, streamlines workflows, and supports faster, more confident decision-making. Designed for high-demand, 24/7 environments of any scale, Security Center is built for scalability, resilience, and cybersecurity - trusted by large, complex organisations that require continuous system availability and rapid threat response.

Key Capabilities

- **Unified Monitoring of Video, Access Control, ALPR, and Communications:** Consolidates video surveillance, access control, automatic licence plate recognition, and communications into a single platform
- **Real-Time Event and Alarm Management:** Enables operators to track access events, review ALPR hits, monitor live video, and respond to alarms from one interface
- **Dynamic Map-Based Visualisation:** Provides interactive facility maps that show device status, operator positions, and live events
- **Integrated Investigation and Reporting Tools:** Allows operators to run investigations, correlate events, and analyse data trends directly within the platform
- **Scalable, Secure System Architecture:** Built-in failover, redundancy, encrypted communications, and flexible integration with hundreds of third-party systems

Approach

Genetec Security Center unifies security with IoT and building systems to give organisations a single operational view that enhances occupancy insight, resource optimisation, and intelligent-building efficiency. Its built-in rules engine automates actions, correlates events, and guides operators through clear, step-by-step responses, improving consistency, speed, and outcomes. Genetec offers deployment flexibility: customers can run Security Center on-premises, within their infrastructure, in the cloud, or as a hybrid solution to match IT strategy and scale.

Video Analytics

IntelexVision

Contact: Charlie Bennett

Email: charlie@intelexvision.com

Website: intelexvision.com



Solution

Sentry is an AI-powered video intelligence platform built to reduce the burden on control room operators and help you act on what actually matters. The platform continuously analyses your camera estate in the background, detecting anomalies and security, safety and operational risks in real time and surfacing only relevant alerts that warrant further attention. Sentry integrates with existing CCTV infrastructure (including VMS, PSIM and camera platforms) so you can add AI contextualisation and analysis without overhauling your setup. The result is faster response times, fewer missed incidents, and a lower false alarm rate, so you can operate with confidence.

Key Capabilities

- Advanced video analytics covering a wide range of security, safety and operational use cases all within a single camera licence – from intrusion detection, to environmental hazards, to missing PPE
- Powerful unusual behaviour engine using self-learning to capture anomalies that would be missed by rules-based analytics
- Generative AI for contextual analysis, forensic investigation of footage, and alert verification
- People and vehicle counting, occupancy analysis and activity heatmapping
- Integrations with existing CCTV infrastructure, including leading VMS, PSIM & camera platforms

Approach

Traditional rule-based analytics generate so much noise that operators stop trusting them, and the burden of vigilance never lifts. Sentry is built on a fundamentally different model. Rather than matching footage against pre-configured rules, the platform learns what normal looks like in your environment and flags what genuinely deviates from it. Alerts are fewer, more relevant, and span a wide range of use cases across security, health and safety, and operations. And because of how it processes video, it scales across large camera estates without prohibitively expensive hardware costs. Making us a trusted video intelligence partner across five continents.

Communications Management | Incident Management Systems

InterTalk Critical Information Systems

Contact: Jeff Kelly

Email: sales@intertalksystems.com

Website: intertalksystems.com



Enlite Cloud-Ready Dispatch

Solution

Enlite is InterTalk's cloud-enabled dispatch console system designed to deliver secure, resilient, and highly accessible control room communications. It enables public safety agencies, government organisations, utilities, transportation, and critical infrastructure operators to manage mission-critical voice and data from virtually anywhere using a secure, browser-based interface. Enlite supports P25 and other industry-standard radio systems whilst integrating seamlessly with CAD, AVL, GIS mapping, video, weather, and other operational tools. Built with geo-diverse redundancy and hybrid deployment options, it ensures operational continuity whether deployed on-premises, hosted, or in a blended environment.

Key Capabilities

- Secure browser-based access: Dispatchers connect via any device on any network – no dedicated hardware or proprietary workstation required.
- Universal communications integration: Connects analogue, digital P25, VoIP, and SIP telephony in a single platform, with direct radio-to-telephone patching.
- GIS and data integration: CAD, AVL, video, weather, and social media feeds combine into a single configurable operational picture.
- 99.999% redundancy: Edge issues detected within one second, with hot standby servers and geo-diverse architecture ensuring continuous operations.
- Vendor-neutral and future-ready: Built exclusively for dispatch, with open interoperability and forward compatibility with MCX and LTE/5G protocols.

Approach

Enlite combines the flexibility of cloud-based access with the proven reliability of InterTalk's mission-critical dispatch heritage. Unlike solutions that force agencies into closed ecosystems, Enlite supports open standards and is built using Commercial-off-the-Shelf (COTS) equipment, helping prevent vendor lock-in. Our hybrid architecture allows agencies to modernise at their own pace whilst maintaining operational control and security. Built to ISO 27001 and ISO 9001 standards and aligned with NIST and OWASP security guidelines, Enlite is engineered for resilience, scalability, and long-term sustainability in high-stakes environments.

Synectics

Email: sales@synecticsglobal.com

Website: www.synecticsglobal.com

SYNECTICS

**Synergy Security and
Surveillance Software**

Solution

Synergy is an integrated security and surveillance software platform designed to bring video, sensors, alarms, and communications into a single, intuitive operational environment. It enables operators to monitor, manage and respond to incidents through a single interface, improving situational awareness and reducing response times. Synergy connects CCTV, access control, analytics and third-party systems, allowing organisations to view events in context and coordinate actions efficiently. The platform is particularly well-suited to complex or high-activity environments where teams must oversee multiple sites or large volumes of information. It is used by public safety organisations, transport networks, critical infrastructure operators, city control rooms, and leisure and hospitality venues.

Key Capabilities

- **Unified System Integration:** Brings together CCTV, access control, alarms, sensors and third-party technologies into a single operational platform
- **Alarm and Event Management:** Consolidates alerts from connected systems and presents them alongside relevant video and contextual data
- **AI-Driven Analytics for Real-Time Risk Detection:** Uses intelligent video analytics to automatically identify unusual activity, potential threats or safety risks
- **Remote Access and Collaboration Tools:** Enables authorised personnel to securely monitor incidents, share information and coordinate actions outside the control room
- **Mapping and Location Awareness:** Provides interactive maps showing cameras, alarms and assets for quick event location and response coordination

Approach

Synectics designs systems that help organisations manage complex security environments without added operational burden. Synergy brings together video, data and analytics from multiple technologies to provide a clearer, connected view of operations. By combining advanced surveillance with AI-driven insight, organisations can move beyond passive monitoring to earlier risk detection, better decisions and more coordinated responses.

Incident Management Systems | Communications Management

Zinc Systems

Contact: Sophie Malone

Email: sophie.malone@zinc.systemsWebsite: www.zinc.systems**Zinc - Incident &
Resilience Platform****Solution**

Zinc's control room solution acts as a unified operational hub that brings incident management, critical communications, tasking and real-time insight together in one intuitive platform. It gives control room teams complete situational awareness by consolidating reporting, alerts, patrols, compliance activities and threat intelligence into a single live dashboard, enabling rapid decision-making and coordinated responses to events. Automated workflows escalate incidents instantly to the right teams and systems, reducing manual handoffs and ensuring consistent, auditable action from report through resolution. Designed for scalability and integration, Zinc can connect with existing control room technology stacks via APIs, to streamline operational processes and synchronise data across tools.

Key Capabilities

- Incident Management: Log, categorise and manage all incidents in one unified system. Structured workflows, media capture and real-time updates ensure faster response. AI summarisation supports incident analysis
- Automated Alerts & Escalation: Rule-based notifications automatically escalate incidents to appropriate teams. Multi-channel communications (App, SMS, email) ensure rapid dissemination of critical information
- Dashboards & Reports: Provides complete situational awareness across incidents and activity. Interactive mapping, geospatial views and heat maps highlight hotspots and emerging risks.
- Tasking & Workflow Automation: Incidents automatically generate structured tasks aligned to predefined SOPs, EOPs and SLAs. Step-by-step guidance embedded directly into workflow with full audit trails
- System Integration & Data Synchronisation: Open APIs enable integration with enterprise systems including body cameras, access control and workplace technology

Approach

Zinc is not just software, it is an operational resilience strategy embedded in technology. Zinc is purpose-built for complex, high-profile estates where compliance, reputation and response speed matter. What truly differentiates us is our DNA: a blended team of technologists and senior security professionals who understand real-world pressure, regulatory scrutiny and board-level accountability. The result is a platform that drives measurable ROI, defensible compliance and intelligence-led decision-making at executive level.

Video Wall & Display Management | Access Control Management | Incident Management Systems

WEYTEC

Contact: Dirk Hendrickx

Email: dirk.hendrickx@weytec.com

Website: www.weytec.com



WDP MX

Solution

In control rooms and trading floors, operators face escalating pressure as they simultaneously manage, control, and monitor multiple systems across high-stakes environments. WEYTEC's flagship product, WDP MX®, is a purpose-built, IP-based KVM (Keyboard, Video and Mouse) platform engineered to address this challenge head-on. WDP MX® stands for "Maximum Experience" and represents WEYTEC's commitment to delivering exceptional levels of performance, usability, flexibility, redundancy, scalability, security, and longevity.

As a unique, IP-based KVM switch solution, WDP MX® enables the shared and simultaneous use of all sources, systems, and content at every workplace, even across multiple locations. Developed entirely in-house by WEYTEC, it integrates and distributes analogue and digital signals from and to systems and video walls within a single, independent IP network.

Key Capabilities

- Operator ergonomics: One keyboard and mouse controls unlimited systems, reducing cognitive load under pressure.
- Collaboration and content sharing: Operators push or pull content between workplaces, screens, and video walls instantly.
- Redundancy and resilience: WDP MX® is configurable from full redundancy to a single cost-efficient system.
- Security and compliance: AES128 encryption, ISO 27001, and NIS2 compliance protect mission-critical environments.

Approach

WEYTEC takes an integrated workplace design approach, going beyond KVM hardware to deliver a single, structured visual environment through its "One Pixel Space" philosophy. Operators interact with multiple sources across freely movable, scalable windows on any screen, with all systems, workplaces, and video walls unified in a single IP network and accessible from any desk or location - reducing cognitive load and supporting faster, more accurate decision-making.



About DG Advisory

DG Advisory helps Directors of Security and executive teams transform mission-critical control rooms into high-performing, resilient operations. We tackle fragmented systems, data overload, and underdeveloped teams by integrating people, process, and technology through proven frameworks and expert design.

Our Control Room Maturity Audit™ provides independent assessment across all seven structural pillars, identifying where operational maturity supports technology investment and where foundations require strengthening first.

For more information: www.dgadvisoryglobal.com



Chris Dreyfus-Gibson MBA MSyl
Managing Director
chris@dgadvisoryglobal.com