

**Deloitte.**



# The cognitive evolution

How AI is transforming Intelligent Command Centers in Saudi Arabia's Giga projects





## Foreword

In an era defined by rapid technological advancement and digital transformation, the integration of Artificial Intelligence (AI) into operational frameworks is not merely a trend but a strategic necessity. Organizations worldwide face the challenge of managing vast infrastructures, increasingly sophisticated systems, and persistent cyber threats. In this context, Intelligent Command Centers (ICCs) have become pivotal. They are more than just technological hubs; they represent a fundamental shift in how organizations approach operational management, security, and strategic decision-making.

The collaboration between Deloitte and Qiddiya in exploring the transformative potential of ICCs highlights the critical importance of innovation and foresight in addressing the complexities of today's digital landscape. Saudi Arabia's Vision 2030, with its ambitious goals for economic diversification and development, provides an ideal environment for pioneering projects such as Qiddiya. As a flagship initiative, Qiddiya is set to become a global destination for entertainment, sports, and culture, demanding exceptional operational intelligence to manage its diverse and dynamic ecosystem.

At the heart of this transformation lies the Intelligent Command Center. By integrating real-time observability, AI-driven automation, and centralized coordination across Digital, IT, Operational Technology (OT) and security environments, ICCs empower organizations to operate smarter, faster, and with greater foresight. They enable leadership to master complexity and convert it into a competitive advantage, ensuring resilience, agility, and market leadership in an increasingly connected and competitive world.



As Chief Technology Officer of Qiddiya, I firmly believe that the integration of AI into our command centers transcends technology alone; it is about transforming our operational strategy to secure resilience, agility, and leadership. In a world where digital complexity and operational risk are ever-present, ICCs provide the cohesive, intelligent, and automated system of control necessary to navigate these challenges.

Abdulrahman AlAli  
Chief Technology Officer, Qiddiya

# Contents

---

<b>Introduction</b>	<b>04</b>
<b>Tracing the evolution of command and control, from traditional analog systems to advanced autonomous solutions</b>	<b>05</b>
<b>Highlighting key considerations organizations must address when strategically planning the implementation of Intelligent Command Centers</b>	<b>15</b>
<b>Defining the problem statement and key challenges to ensure successful implementation of the Intelligent Command Center</b>	<b>19</b>
<b>Exploring the role of AI in enhancing the capabilities and effectiveness of the Intelligent Command Center</b>	<b>26</b>
<b>The ICC market in KSA is rapidly growing, driven by strategic investments and increasing demand for advanced operational capabilities</b>	<b>32</b>
<b>Case Study - Qiddiya Investment Company, KSA</b>	<b>35</b>
<b>References</b>	<b>59</b>
<b>Glossary of terms</b>	<b>60</b>

## Introduction

In today's hyper-connected and high-stakes digital environments, organizations must manage vast infrastructures, increasingly complex systems, and constant cyber threats. Traditional monitoring tools and reactive operational approaches are no longer sufficient. The Intelligent Command Center (ICC) represents a transformative solution. It is not just a technology platform but a strategic capability — one that integrates real-time observability, AI-driven automation, and centralized coordination across Digital, IT, OT, and security environments. By enabling organizations to operate smarter, faster, and with greater foresight, the ICC empowers leadership to take control of complexity and turn it into a competitive advantage.

### **What is the solution of an ICC?**

Integrated platform that delivers end-to-end observability, monitoring, operational control across infrastructure, applications, network security, and smart devices. By consolidating telemetry and operational data from multiple sources into a single unified environment, the ICC enables real-time correlation, analysis, and response to enhance resilience, security, and operational efficiency.



# Tracing the evolution of command and control, from traditional analog systems to advanced autonomous solutions

The transformation of command and control is an evolution from manual-to-digital to truly intelligent. This journey can be witnessed across three eras.

### **Era of analog and automation (1980s - early 2000s)**

**The challenge:** Traditional control rooms were driven by manual processes, physical checklists, and operators reacting to alarms and phone calls. Response was reactive and often delayed, dependent on human vigilance and manual coordination. Situational awareness was limited to what operators could observe or be told, with no real-time synthesis of information. Security and operational data were substantially disconnected.

**The first digital step:** Early automation platforms digitized alarm responses, connecting an event to a predefined procedure reducing human error and speeding up reaction times. This was a critical step in minimizing response delays and standardizing operations.

**Core capability:** Digital response automation executes decisions that have already been made. Operators still needed to interpret data and make strategic decisions.

### **Era of centralization and advanced analytics (2000s - early 2020s)**

Command centers underwent a significant transformation by becoming centralized hubs that consolidated multiple security and operational systems into a single, cohesive platform. Systems such as video surveillance, access control, intrusion detection, and IT monitoring were integrated into unified dashboards, allowing operators to access and manage diverse streams of information from one place. This centralization provided a holistic view of the organization's overall security posture and operational status, greatly enhancing coordination among teams and improving situational awareness. As a result, operators were better equipped to understand complex scenarios in real time and respond more effectively to emerging threats or incidents.

**The data challenge:** The sheer volume of data, especially from early video motion detection, led to an unacceptable number of "false positives." This required human operators to spend their time filtering noise rather than analyzing threats.

**The solution:** The introduction of Advanced Video Analytics and early Machine Learning (ML) models to accurately detect people, objects, and anomalies, making large-scale monitoring practical for the first time.

**Core capability:** Real-Time Situational Awareness (Presenting complex data for human analysis). Operators remained central to interpreting insights and initiating responses. <sup>1</sup>



## The era of cognitive command: AI and Generative AI (GenAI) (today and beyond)

**The paradigm shift:** The Intelligent Command Center (ICC) is no longer a monitoring station; it is an autonomous decision-support system. AI technologies enable the command center to not only detect events but also understand context, predict outcomes, and recommend or execute actions. This is where AI moves beyond simple automation to truly intelligent decision-making.

**The AI differentiator:** AI and GenAI can process structured and unstructured data (text, images, signals) at a scale and speed impossible for humans. It actively detects subtle patterns, forecasts potential outcomes, and even generates recommended courses of action.

**The new role for humans:** Human operators transition from routine responders to strategic overseers and ethical guardians. They collaborate with AI "virtual operators" that handle routine decision-making and alert prioritization. The ICC handles routine decision-making, freeing human experts for strategic initiatives and ethical oversight.

**Core capability:** The ICC supports or autonomously makes decisions based on real-time data, predictive analytics, and AI reasoning. This leads to faster, more accurate, and context-aware responses. The system continuously learns and adapts, improving over time.<sup>1</sup>

The journey from the Era of Analog to the Era of Cognitive Command shows a clear trend: the increasing dependence on automated intelligence to manage complexity. This evolution has pushed the capabilities of command centers far beyond their original design, creating an operational landscape defined by real-time data integration, predictive analytics, and autonomous decision support.

However, the rapid acceleration of AI deployment also introduces significant market dynamics—chief among them, unrealistic expectations versus tangible, scaled deployment. To gauge the current maturity and potential volatility of the specific AI technologies driving this

transformation, we must move from a historical perspective to a market-based assessment.

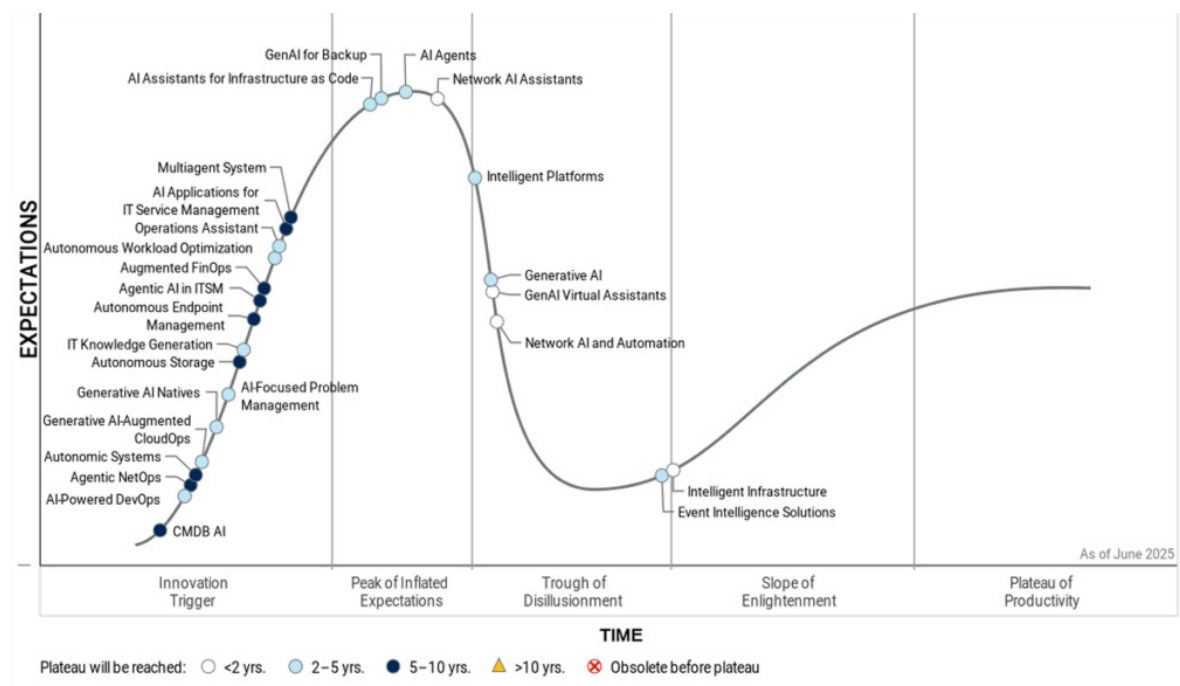
This is precisely where the Gartner Hype Cycle becomes a good reference tool. It provides an essential snapshot of which technologies—the advanced analytics, machine learning agents, and intelligent automation platforms discussed previously—are nearing true enterprise value and which are still navigating the initial peak of inflated expectations or the subsequent trough of disillusionment. Understanding this cycle is vital for any organization planning their roadmap for the Intelligent Command Center of the future.

# Examining the Gartner Hype Cycle for AI in IT Operations through the lens of the Intelligent Command Center

The Gartner Hype Cycle for AI in IT Operations focuses on how Artificial Intelligence is being applied to automate and enhance operational monitoring, incident management, and infrastructure performance — the technical foundation of any command center environment. For intelligent command centers, this cycle captures the shift toward autonomous IT operations where AI-driven systems handle event correlation, anomaly detection, root cause analysis, and self-healing automation across hybrid and cloud environments. AIOps technologies integrate with telemetry, logs, and observability tools to filter noise, prioritize alerts, and recommend or execute remediation steps. Within a command center, this means AI can monitor thousands of signals across systems, identify early indicators of degradation or threats, and orchestrate a coordinated response — often before service users are affected. Over time, Artificial Intelligence for IT Operations (AIOps) platforms learn from human operator decisions, refining their predictive accuracy and operational response models.

The AIOps Hype Cycle contextualizes how intelligent command centers evolve from static dashboards to dynamic, self-learning operational ecosystems, where AI continuously optimizes performance, reliability, and incident response across complex digital infrastructures.<sup>2</sup>

## GARTNER HYPE CYCLE FOR AI IN IT OPERATIONS - 2025



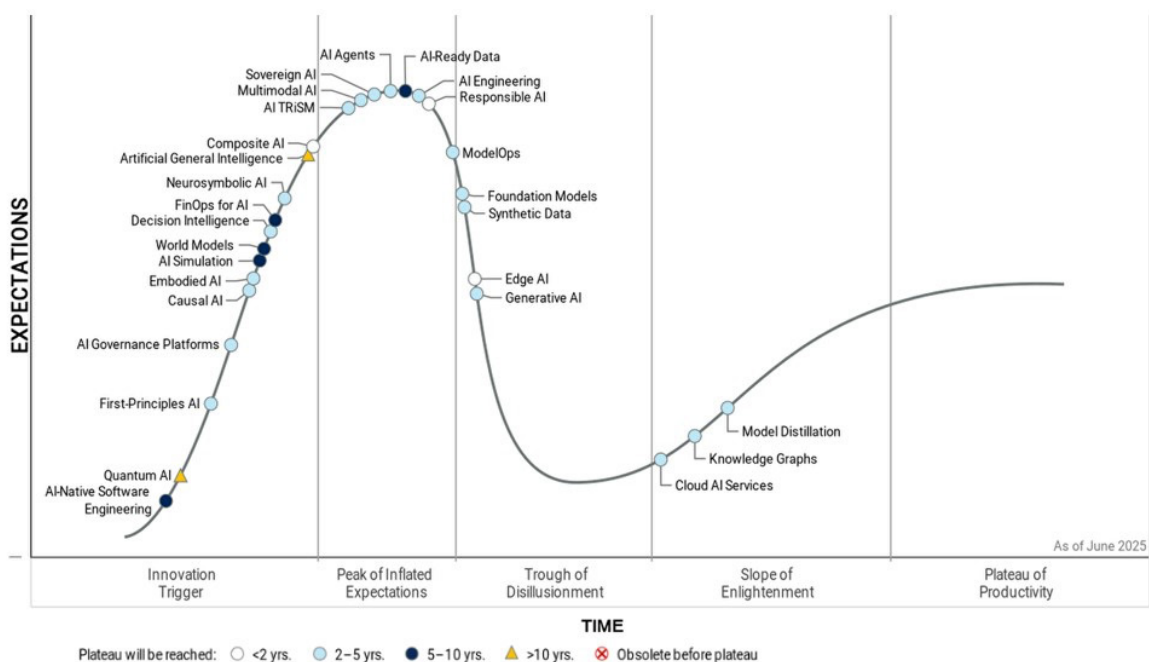


# Exploring Gartner's Hype Cycle for Artificial Intelligence from the Intelligent Command Center perspective

The Gartner Hype Cycle for Artificial Intelligence illustrates the maturity and adoption of AI technologies that underpin the intelligence layer within modern command centers. It charts how innovations such as machine learning, natural language processing, decision intelligence, autonomous agents, and knowledge graphs progress from experimentation to enterprise-scale deployment. In the context of intelligent command centers, this Hype Cycle provides a lens into how AI is transforming situational awareness, real-time decision support, predictive analytics, and automated response orchestration. Many command centers now rely on AI systems capable of integrating data from sensors, networks, and human inputs to generate insights and recommendations faster than human operators could alone. Technologies featured in this Hype Cycle — such as GenAI, Agentic AI, and multimodal analytics — are enabling command centers to move from reactive monitoring toward anticipatory operations, where systems can detect anomalies, forecast incidents, and coordinate actions autonomously.

The AI Hype Cycle situates intelligent command centers within the broader transformation of decision-making systems — from manual, human-led analysis to AI-augmented operational intelligence capable of interpreting complex, real-time data at scale.<sup>3</sup>

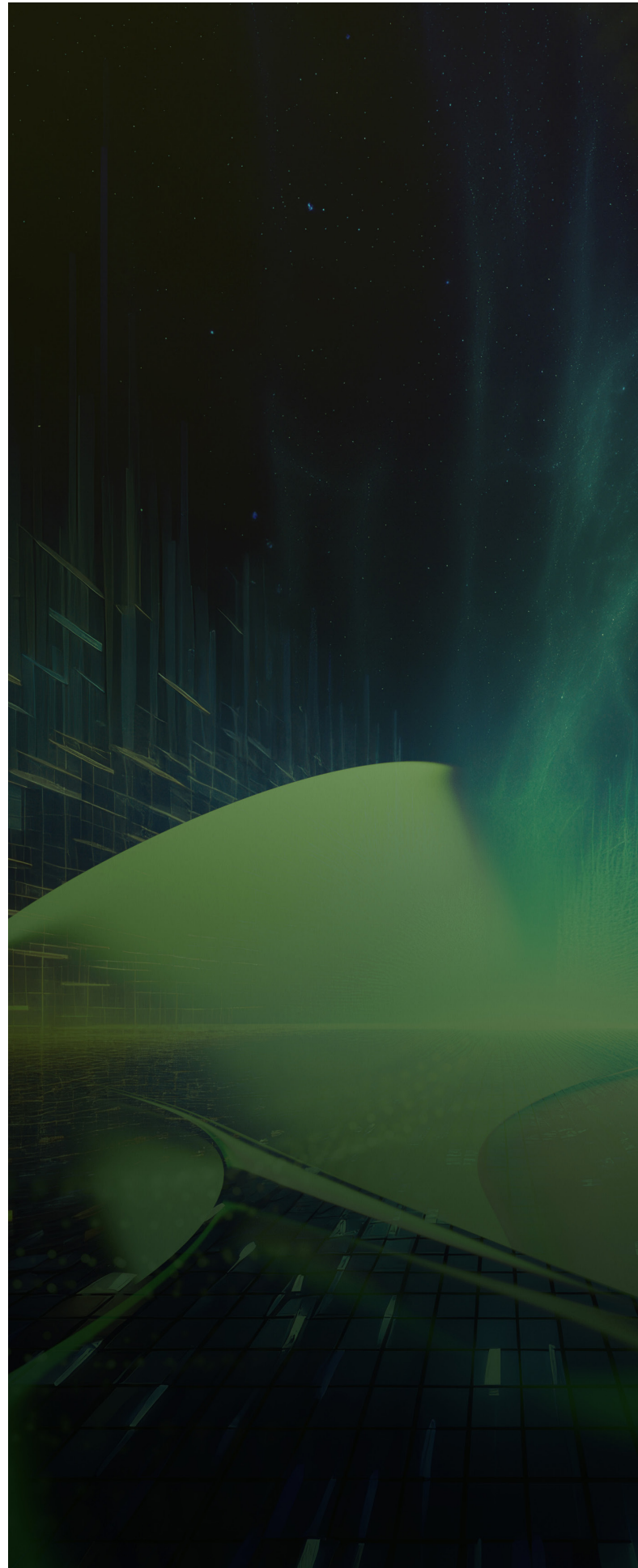
## GARTNER HYPE CYCLE FOR ARTIFICIAL INTELLIGENCE - 2025



The Gartner Hype Cycle serves as a stark reminder that simply adopting a technology at its "Peak of Inflated Expectations" does not guarantee success. For Intelligent Command Centers to move beyond experimental projects and realize the full "Plateau of Productivity," they must overcome the challenges of complexity, lack of operational reliability, and, critically, a deficit of trust in autonomous decision-making.

This is where the focus shifts from what AI technologies are available to how they are architected, governed, and deployed.

The pathway to sustainable, scalable intelligence requires a pivot to Agent Operations (AgentOps). AgentOps is the new architectural and operational paradigm that standardizes the development, deployment, and lifecycle management of sophisticated AI systems, or "agents," that work collaboratively to run the command center. It is the architectural answer to the Hype Cycle, providing the essential backbone for achieving automation, explainability, and observability at scale.





# Understanding modern AgentOps as a key enabler for automation, explainability, and observability within intelligent IT operations

## Three layers of modern AgentOps

Leading-edge AgentOps platforms are built upon three essential pillars that collectively enable intelligent, secure, and efficient agent management:

---

### AI layer

This pillar serves as an AI agent-driven distributed orchestrator. It empowers organizations to securely build, deploy, and manage the entire lifecycle of AI agents while enforcing strict guardrails and quality controls. By seamlessly integrating a diverse range of large and specialized AI models, curated datasets, and automation tools, the AI Layer drives sophisticated, autonomous workflows that adapt to complex operational needs.

---

### Data layer

Acting as a comprehensive data consolidation layer, the Data Layer aggregates and harmonizes information from multiple, often disparate, sources. It creates a unified, reliable foundation that supports informed decision-making by agents. Utilizing advanced technologies such as graph databases and knowledge graphs, this fabric maps and understands the relationships between various system components, enabling context-aware and intelligent agent actions.

---

### Automation layer

This layer provides the execution framework that allows agents to carry out their decisions effectively across the entire IT ecosystem. It delivers robust workflow automation capabilities, including rollback mechanisms and resilient to errors or interruptions.<sup>4</sup>

## Explainability and observability features

Modern AgentOps platforms place a strong emphasis on transparency and insight into agent behavior by incorporating the following features:

**Comprehensive storyboards:** Visual narratives that offer clear, step-by-step visibility into how agents operate, enabling stakeholders to understand workflows and outcomes intuitively.

**Detailed metrics:** Quantitative data tracking key performance indicators such as the number of agent executions, alerts analyzed, tickets generated and realized cost savings. These metrics provide measurable evidence of agent effectiveness and impact.

**Outage prevention tracking:** Continuous monitoring mechanisms that identify potential system disruptions early, demonstrating the platform's proactive value in maintaining operational stability.

**Task-level execution visibility:** Granular insight into each individual task performed by agents, allowing for precise monitoring and troubleshooting of automated processes.

**Decision point documentation:** Clear records of critical decision moments, including the rationale behind each choice, which supports accountability and facilitates auditability.

**Full audit trails:** Comprehensive logs capturing every automated action taken by agents, ensuring traceability and compliance with regulatory or organizational standards.<sup>4</sup>



## Security and governance architecture

To safeguard operations and maintain trust, these platforms incorporate stringent security and governance frameworks, including:

---

### AI guardrails

Pre-execution validation mechanisms that review and approve all agent actions, preventing unintended or harmful behaviors before they occur.

---

### Privilege management

Strict controls over who can access data and perform actions, ensuring that agents operate within authorized boundaries only.

---

### Role-Based Access Controls (RBAC)

Defined roles that limit agent capabilities according to user responsibilities, reducing risk by enforcing the principle of least privilege.

---

### Comprehensive security policies

Well-defined rules and protocols that govern agent behavior, ensuring consistent adherence to organizational and regulatory requirements.

---

### Privacy protections

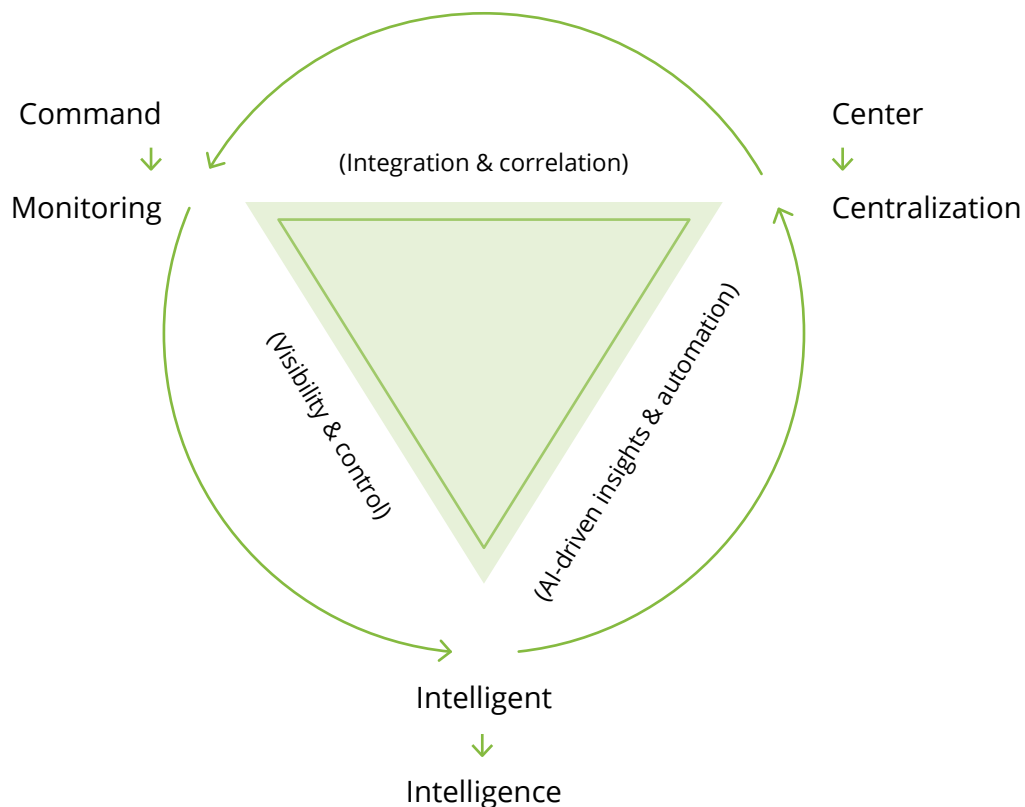
Measures designed to safeguard sensitive operational data from exposure or misuse, maintaining confidentiality and compliance with data protection standards.<sup>4</sup>



## What makes a Command Center Intelligent?

A Command Center transitions from a traditional, reactive monitoring room to an **Intelligent Command Center (ICC)** by moving beyond simply displaying data. Intelligence is achieved through the systematic integration of advanced AI capabilities that enable the center to anticipate, reason, and act autonomously or semi-autonomously.

The fundamental shift is from "monitoring and responding" to "predicting and preventing."



An Intelligent Command Center serves as the organization's "Cognitive Brain," integrating monitoring, visibility, and control through centralized systems. By leveraging management platforms and AI-driven intelligence, it processes information at a speed and scale beyond human capability, enabling smart automation and informed decision-making. This empowers teams to concentrate on strategic oversight and complex problem-solving.

# Highlighting key considerations organizations must address when strategically planning the implementation of Intelligent Command Centers

# Addressing how organizations often confuse hype with strategic value in technology adoption

Trends are defined as measurable, sustained changes that develop over time, rather than fleeting headlines or short-lived technology fads that capture attention temporarily. However, many organizations fall into the trap of pursuing these “shiny objects” — popular but superficial innovations — instead of recognizing and responding to genuine strategic signals.

This challenge becomes even more pronounced when companies focus solely on trends within their own industry. Such a narrow view limits their perspective and prevents them from seeing important shifts occurring at the intersections of different sectors. True disruption rarely arises from a single trend in isolation; rather, it emerges from the convergence of multiple forces across diverse domains.

By consistently monitoring the right trends and analyzing their wider implications beyond immediate industry boundaries, organizations can enhance their ability to anticipate future developments. This improved foresight enables them to make more informed, strategic decisions that drive long-term success.

## **Defining trends: What organizations can truly know**

Trends represent measurable changes that unfold over time, supported by solid data and thorough research. They are observable patterns that demonstrate consistent movement in a particular direction, rather than random or isolated events. Unlike fleeting opinions or assumptions, trends are developments that can be tracked, quantified, and validated through reliable evidence. This makes them a dependable foundation for organizations to base their strategic planning and decision-making on.

## **Understanding uncertainties: What organizations cannot predict**

Uncertainties refer to future conditions that cannot be precisely predicted or measured. They involve variables that may evolve in several different directions, making their outcomes inherently unpredictable. Even with careful analysis and extensive data, certain events remain unknown and cannot be forecasted with certainty. Recognizing these uncertainties is crucial for organizations, as it highlights the limits of foresight and the need for flexible, adaptive strategies to navigate unpredictable environments.<sup>5</sup>



The Future Today Strategy Framework helps leaders navigate complexity and make strategic decisions in a world of rapid change

### Strategic horizon scanning

Identify which emerging technologies and trends will directly impact your organization's growth and evolution in the next 12-36 months.

### Risk & disruption mapping

Plot potential disruptions from both expected and unlikely sources. Rather than traditional risk assessment, focus on how technological convergence could create unexpected competitive threats or market opportunities.

### Organizational readiness

Evaluate your current capabilities against future requirements. This isn't just about technology adoption — it's about assessing if your culture, talent, and processes can adapt to and thrive in rapidly evolving market conditions.

### Action planning

Transform insights into executable strategies. Move beyond traditional strategic planning to create dynamic response frameworks that allow your organization to pivot quickly as technological changes accelerate or decelerate.<sup>5</sup>

# Today's science and tech advances are revealing how much we don't understand about our own potential.

# Emphasizing the importance of imagining the future as a critical element of effective foresight

Imagining the future is central to the practice of foresight, especially during times of uncertainty when clarity is crucial. This process is impactful because it encourages us to think beyond our usual assumptions and instinctive ideas. By doing so, it enhances our creative thinking about potential opportunities and challenges. This imaginative exercise supports setting a strategic direction and informs the actions we take today to prepare for tomorrow.

## The role of scenarios in imagining the future

A key part of imagining the future involves developing scenarios—structured narratives or models that describe possible future states. Scenarios help us explore different ways the future might unfold, which aids in strategic planning and decision-making.

## Types of scenarios

Scenarios generally fall into three broad categories:

### Predictive scenarios

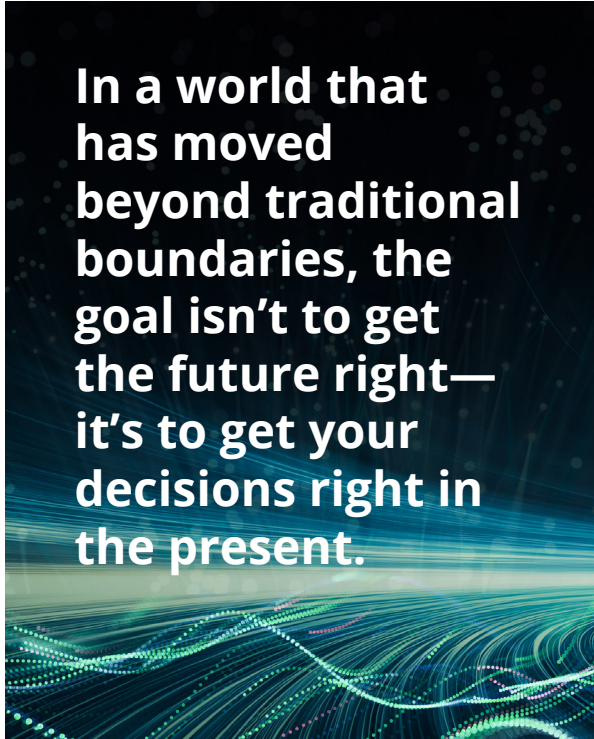
These focus on forecasting the future based on current information and trends. They aim to develop outlooks grounded in what is known today, often relying on data and statistical methods to predict likely outcomes.

### Exploratory scenarios

These define a range of possible futures based on different assumptions and driving forces. Rather than predicting one outcome, exploratory scenarios consider multiple possibilities, helping to understand how various factors might interact to shape the future.

### Normative scenarios

Positioned between predictive and exploratory types, normative scenarios incorporate both current information and desired future goals. Their purpose is to identify pathways to achieve preferable futures. This process is often called backcasting, where one starts with a desired future and works backward to determine the steps needed to reach it.<sup>6</sup>



**In a world that has moved beyond traditional boundaries, the goal isn't to get the future right—it's to get your decisions right in the present.**



# Defining the problem statement and key challenges to ensure successful implementation of the Intelligent Command Center



## Problem statement

Lack of observability and monitoring to ensure 24x7 availability, seamless operations, and proactive issue resolution across its IT and OT systems, resulting in fragmented monitoring, delayed response, suboptimal performance, and inconsistent service delivery.

## Key challenges in modern IT environments

### Distributed infrastructure

Today's organizations operate across a complex and distributed infrastructure that spans on-premise data centers, multiple cloud platforms, and edge computing environments. Managing this diverse ecosystem requires seamless integration and coordination to ensure consistent performance and security across all locations.

### Accelerated business processes

Business operations increasingly rely on continuous, 24/7 digital availability. Any downtime or disruption can have immediate and significant impacts on productivity, customer satisfaction, and revenue. This acceleration demands resilient systems and proactive management to maintain uninterrupted service.

### Growing user demands

Users expect experiences that are not only seamless and fast but also secure and personalized to their needs. Meeting these rising expectations requires sophisticated technology solutions that can adapt dynamically while safeguarding privacy and data integrity.



### Sophisticated cyber threats

As critical infrastructure becomes more interconnected, it also becomes a prime target for increasingly sophisticated cyber attacks. Organizations must defend against a wide range of threats that can compromise operations, data, and trust.

### Shortage of skilled personnel

Managing hybrid IT and Operational Technology environments demands specialized skills that are in short supply. This talent gap challenges organizations to find new ways to optimize resources, automate routine tasks, and upskill existing teams.

### Managing applications in complex multicloud environments

Modern approaches have introduced significant complexity, making it challenging for IT and security teams to manage their applications efficiently. The dynamic nature of multicloud environments generates an overwhelming volume of data that exceeds human capacity to collect, analyse, and respond to effectively. Consequently, teams find it difficult to obtain the insights necessary to accelerate innovation while maintaining security, which ultimately slows down their progress.

## IT and security teams find it increasingly difficult to monitor and manage their applications



In this complex landscape, organizations require more than just visibility into their systems—they need intelligent situational awareness that provides real-time insights and context, combined with orchestrated control to respond swiftly and effectively. This is precisely the role of the Intelligent Command Center (ICC), which integrates these capabilities to enable proactive, coordinated management of modern digital environments.<sup>7</sup>

## Identifying the key operational challenges enterprises face today and their impact on business performance and growth

Despite significant advances in monitoring technologies and automation, many organizations continue to face persistent operational difficulties:

### Fragmented visibility

Data remains scattered across multiple tools, teams, and environments, making it difficult to obtain a unified, comprehensive view of operations. This fragmentation hampers effective monitoring and timely decision-making.

### Delayed detection and response

Incident triage and response processes often take hours or even days, increasing the risk of prolonged disruptions and greater damage. Slow reaction times undermine operational resilience and customer trust.

**77%**



of technology leaders are involving more teams from outside of IT in making decisions using observability-driven insights to drive greater value

**86%**



of technology leaders say cloud-native technology stacks produce an explosion of data that is beyond humans' ability to manage<sup>7</sup>



### Manual and reactive workflows

Operational teams are frequently burdened by repetitive, manual tasks that limit their capacity to focus on strategic initiatives. This reactive approach reduces efficiency and increases the likelihood of errors.

### Cybersecurity blind spots

As digital ecosystems grow more complex, attack surfaces expand, creating vulnerabilities that are difficult to detect and defend against. Organizations struggle to maintain comprehensive security coverage across all assets.<sup>8</sup>

**In 2025, the global average cost of a data breach reached \$4.44 million with the highest in the US at \$10.22 million, followed by the Middle East at \$7.29 million<sup>9</sup>**

**One in four cyberattacks involved ransomware, with a 143% increase in ransomware victims worldwide in early 2023<sup>8</sup>**

**The annual global cost of ransomware attacks is projected to escalate reaching \$265 billion by 2031<sup>8</sup>**

# Highlighting the cost of inaction and demonstrating the transformative power of the Intelligent Command Center in driving business success

## Impact of doing nothing

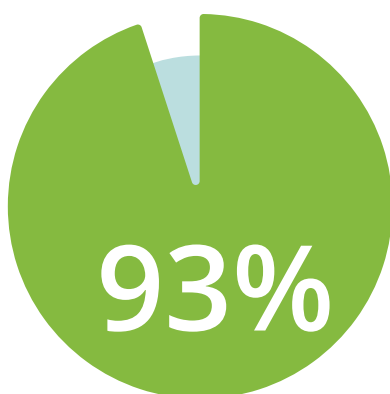
The organization will continue to face fragmented visibility across IT and OT systems, leading to higher risk of unplanned outages, longer incident resolution times, inefficiencies in operations, escalating operational costs, and inability to guarantee seamless service delivery and performance expectations. which may affect guest experience and security.

## By implementing an Intelligent Command Center

### Reduce impact of incidents

Improve early detection allowing teams to prevent incidents before they have an impact on operations thereby enhancing guest experience and security

Intelligent correlation of events and advance root cause analysis, allowing for a reduction in resolution time per incident



of organizations have or will adopt AIOps to reduce the complexity of managing their multicloud environment within the next 12 months

### Increase reliability maturity

Ally throughout the entire application lifecycle, allowing early issue detection in source code to avoid incidents and vulnerabilities during production thereby enhancing overall security

Digital Experience Monitoring capabilities, to understand how guest and employees interact with the organization application landscape supporting the enhancement of guest experience

Better understanding of the IT Stack, including system integration requirements and the performance of in-place solutions

Rendering development pipelines secure and optimizing the response to patch the affected systems by operations

Health check activities, reducing operating cost as these activities used to be carried out by human operators

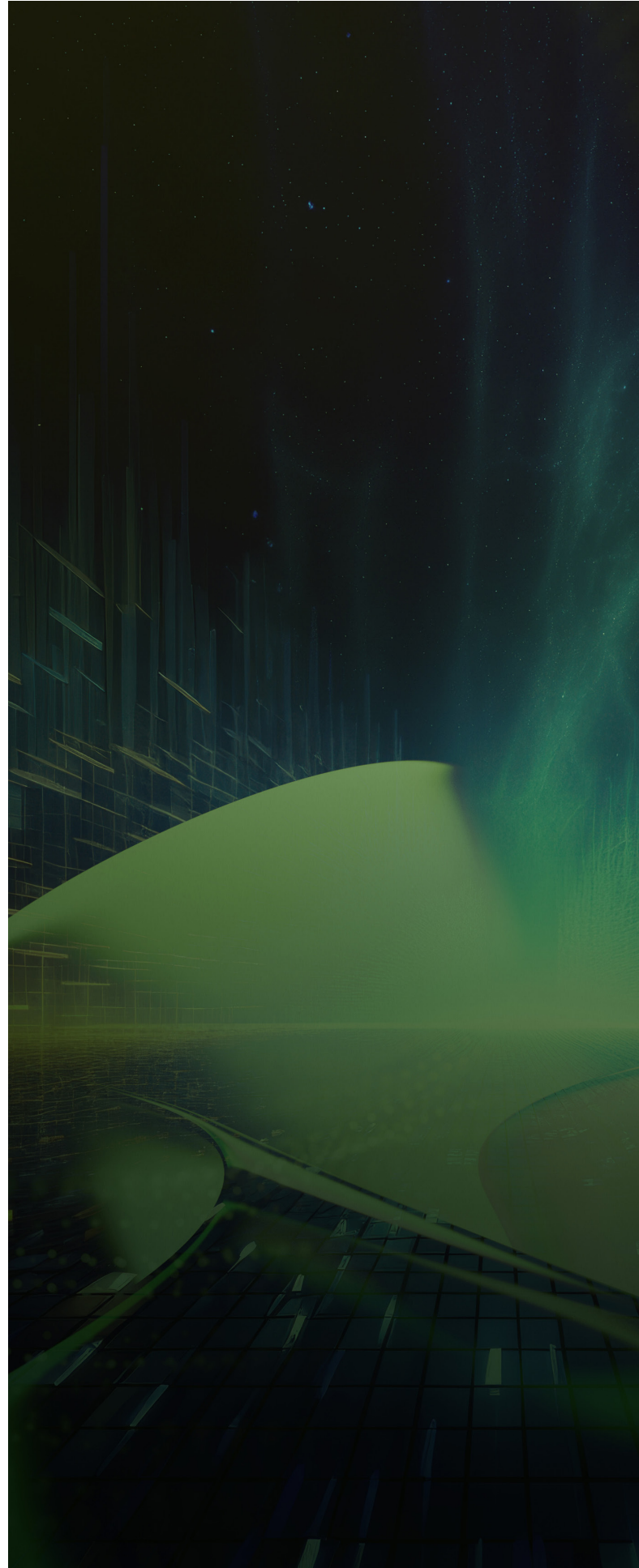
Automated auto-healing playbooks allow to reduce human interaction in issue resolution, improving uptime

Shift operations from a reactive to preventive one, detecting optimal maintenance windows and reducing operational overhead<sup>8</sup>

The severe penalties—ranging from catastrophic system failures and operational paralysis to reputational damage and human safety risks—underscore that inaction is no longer an option.

To neutralize these escalating threats, the Intelligent Command Center must adopt a proactive, cognitive posture. This is precisely where Artificial Intelligence steps in as the essential antidote, enhancing the core capabilities of the ICC to directly target and mitigate the root causes of these risks: data overload, delayed decision-making, and human error.

By improving real-time monitoring and rapid response, the ICC also helps maintain a seamless guest experience and strengthens security measures throughout the facility.





# Exploring the role of AI in enhancing the capabilities and effectiveness of the Intelligent Command Center



# Leveraging AI to drive transformative growth through agile and scalable operational capabilities

## Speed is the new scale

Artificial Intelligence is fundamentally transforming how organizations make decisions by dramatically compressing decision cycles — from weeks or months down to minutes or even seconds. This acceleration shifts competitive advantage towards those organizations that can effectively leverage AI for rapid experimentation, continuous learning, and agile adaptation. However, speed alone is not enough. Success depends on making sound strategic choices around data governance to ensure quality and compliance, careful vendor selection to align with organizational goals, and robust change management to embed AI-driven processes smoothly into existing workflows.

## The middle office is melting

AI is increasingly automating the coordination, oversight, and decision-making tasks traditionally performed by human intermediaries in the middle office. These roles, which often involved manual approvals and complex communication chains, are being replaced by intelligent systems capable of faster, more consistent execution. Organizations that resist this shift by maintaining manual coordination and approval processes risk becoming structurally inefficient and uncompetitive. The emerging organizational model is one that is flatter, more agile, and capable of faster response times, driven by AI-enabled automation.

## Scale out over scale up

Historically, core technologies tend to become more affordable and widely accessible over time, leading to decentralization and distribution. AI is following this same trajectory. While some companies focus on building ever-larger models and massive data centers, they risk being outpaced by more nimble competitors who deploy smaller, more efficient AI systems that are quicker to implement and less costly to operate. The future belongs to organizations that prioritize scaling out—distributing AI capabilities broadly and efficiently—rather than simply scaling up infrastructure size.<sup>5</sup>

# How Intelligent Command Centers leverage AI to effectively overcome operational challenges

The Intelligent Command Center leverages the power of Artificial Intelligence to deliver critical capabilities that directly address the complexities and challenges faced by modern organizations:

## Predictive analytics

AI enables the ICC to anticipate potential threats, system failures, and operational challenges before they occur. By analyzing vast amounts of data in real time, predictive analytics allow organizations to take proactive measures, reducing downtime and mitigating risks effectively.

## Automated workflows

AI-driven automation streamlines routine and complex processes, significantly reducing the need for manual intervention. This not only enhances operational efficiency but also frees up skilled personnel to focus on higher-value tasks.

**Globally, task automation currently stands at 34%, a slight increase from 33% in 2020, though still below earlier forecasts of 47% by this time. Looking ahead, businesses expect task automation to reach 42% by 2027, with approximately 35% of these automated tasks involving decision-making and 65% focused on data processing. In contrast, automation of reasoning and communication tasks is projected to grow more modestly, by around 9% by 2027.<sup>10</sup>**

## Enhanced decision-making

Beyond automation, AI supports strategic decision-making by generating innovative solutions, simulating scenarios, and providing actionable insights. This empowers organizations to respond more effectively to dynamic conditions and complex challenges.



# Understanding the global shift towards integrated command centers and its impact on organizational operations

The world is increasingly adopting Integrated Command Centers due to significant technological advances and a universal demand for greater efficiency, safety, and resilience. This trend spans multiple sectors, including public safety and defense (Command and Control or C2), logistics (Control Towers), and enterprise operations.

Global trend	AI/ML application in the ICC	Core benefit
GenAI & Natural Language Processing (NLP)	NLP enables human operators to interact with complex data using voice or text commands (e.g., "Show me all the current risk zones in the Western Sector."). GenAI can instantly summarize large volumes of incident reports	Faster access to information and improved collaboration between humans and machines
Predictive & Proactive Operations	Uses AI to predict equipment failures, perform predictive maintenance, and forecast supply chain disruptions by analyzing diverse data sources such as social media sentiment and weather patterns	Significant reduction in downtime and proactive allocation of resources
Agentic AI & Autonomous Systems	AI agents work together to process data from multiple sources (drones, satellites, sensors) and recommend complex, multi-step responses. This approach evolves beyond simple automation to adaptive, collaborative systems.	Enhanced resilience, faster responses, and improved decision-making at the operational edge
Augmented Reality (AR) Interfaces	AI-generated real-time insights are overlaid onto the physical environment (e.g., AR glasses showing status on-site)	Increased maintenance efficiency and quicker decision-making during operations
Holistic Governance and Compliance	Centralized AI Control Towers monitor AI model performance, enforce company-wide AI policies, and maintain automated, tamper-proof audit trails.	Lower legal risks, ensured regulatory compliance, and optimized AI-related costs.

## The result is a measurable impact, reflected in improved efficiency, faster decisions, reduced risks, and clear business value

Implementing an Intelligent Command Center approach, experience several measurable and impactful benefits that go beyond technical improvements. These outcomes demonstrate the ICC's role as a vital business enabler.

---

### Up to 70% reduction in incident resolution times

By centralizing monitoring and response activities, the ICC approach streamlines incident management processes. This leads to significantly faster identification, diagnosis, and resolution of issues, reducing the time incidents remain unresolved by up to 70%. Faster resolution minimizes disruption and helps maintain business continuity.

---

### Higher customer satisfaction due to service stability and responsiveness

Customers benefit from more stable and reliable services, as well as quicker responses to any issues that arise. This leads to improved customer trust and satisfaction, which are critical for long-term business success.

---

### Significant decrease in downtime and revenue loss from service outages

With improved incident response and proactive monitoring, organizations experience fewer and shorter service outages. This reduction in downtime directly translates into less revenue loss and protects the organization's reputation by ensuring services remain available and reliable.

**Up to 50% reduction in unplanned outages through predictive maintenance<sup>11</sup>**

---

## Improved cybersecurity posture with proactive threat management

The ICC approach incorporates continuous threat detection and response capabilities. This proactive stance helps organizations identify and mitigate cybersecurity risks before they escalate into serious breaches, strengthening overall security resilience

**Instant anomaly detection across complex IT, physical, and operational environments**

---

## Enhanced visibility across departments, systems, and third-party services

The ICC provides a unified view of operations, integrating data from various departments, internal systems, and external third-party services. This comprehensive visibility enables better coordination, quicker decision-making, and more effective management of complex environments.

**20-40% improvement in worker productivity by automating repetitive tasks**

The worldwide momentum for Intelligent Command Centers—driven by the imperative for predictive resilience — is not occurring in a vacuum. It is fundamentally reshaping national strategies and regional competitiveness. The global trends we have identified, particularly the move towards highly automated and cognitively enabled operations, are serving as a strategic blueprint for nations seeking to diversify their economies.

Nowhere is this phenomenon more pronounced than in the Kingdom of Saudi Arabia. For KSA, the rise of the ICC is not merely an IT upgrade; it is a core pillar of the national transformation agenda, Vision 2030. The Kingdom is actively embracing these global standards, viewing AI and sophisticated data management as the principal levers for economic diversification, public safety enhancement, and the creation of the world's most advanced urban and industrial megaprojects.<sup>12</sup>



# The ICC market in KSA is rapidly growing, driven by strategic investments and increasing demand for advanced operational capabilities

The Kingdom of Saudi Arabia has made AI and Data central to Vision 2030. This ambitious vision is driven by key government bodies such as the Saudi Data & AI Authority (SDAIA), which is orchestrating one of the world's most comprehensive and aggressive national deployments of intelligent command capabilities.<sup>1</sup>

In parallel, Saudi Arabia is investing heavily in building AI capacity and human capital. The establishment of the National Center for AI (NCAI) is a key part of this effort, focusing on AI research, development, and deployment. Additionally, initiatives such as the AI Scholarship Program are designed to cultivate a skilled workforce capable of designing, operating, and strategizing within these new cognitive environments. This focus on education and training ensures that the Kingdom has the expertise necessary to sustain and grow its AI capabilities over the long term.



## AI in critical infrastructure and operations

The application of intelligent command centers (ICCs) in Saudi Arabia extends far beyond traditional security functions, encompassing critical sectors that are vital to the success of Vision 2030's megaprojects. In the realm of smart city operations, projects such as NEOM and the Red Sea Project are pioneering the concept of cities managed entirely through intelligent control centers. These centers leverage extensive networks of Internet of Things (IoT) sensors to collect real-time data on traffic flow, resource consumption such as water and energy, and public safety. AI-driven predictive models are used to optimize traffic management, reduce resource waste, and anticipate safety risks, enabling proactive and efficient urban management.<sup>13</sup>

**In healthcare**, King Faisal Specialist Hospital & Research Center (KFSHRC) has deployed a Capacity Command Center powered by AI and Evidence-Based Practices (EBP). This center focuses on measuring and managing adherence to clinical and operational guidelines, monitoring healthcare services, and improving process mapping to identify inefficiencies. By implementing new processes informed by AI insights, the hospital aims to maximize capacity utilization and enhance patient outcomes. This AI-driven approach supports data-informed decision-making and operational efficiency in healthcare delivery.<sup>14</sup>

**Industrial safety and project control** are also critical areas where AI-powered Safety Command Centers (SCCs) are being deployed. Given the scale and complexity of Saudi Arabia's mega-projects, these centers use AI-powered video analytics to monitor high-risk environments such as construction sites and oil and gas fields. Real-time compliance monitoring allows for the detection of unsafe behaviors and machinery non-compliance without continuous human supervision. This technology significantly improves worker safety and overall project management by reducing the risk of accidents and ensuring adherence to safety standards.<sup>15</sup>

**In the energy and resources sector**, AI platforms are used to unify operational data from oilfield operations. These platforms enable real-time anomaly detection and predictive maintenance, which help optimize resource allocation and reduce downtime. The integration of AI in energy management supports the Kingdom's goals of sustainable resource use and maximized productivity, contributing to the efficient operation of one of its most important economic sectors.<sup>11</sup>



## The ultimate testbed: Qiddiya's Intelligent Command Center

To understand the tangible application of cognitive control and predictive resilience, one must look to the Kingdom's Giga Projects, which are being built as natively smart environments. Among them, Qiddiya City offers a unique and compelling case study.

Qiddiya is more than an entertainment, sports, and culture destination; it is a purpose-built, high-density, dynamic ecosystem that exemplifies the most complex operational challenges facing any modern smart city:

**Massive scale & dynamic flow:** It is a high-volume venue designed to attract millions of visitors annually, with constantly shifting crowds, event schedules, and critical infrastructure needs—a perfect environment for testing real-time operational resilience.

**Digital native infrastructure:** Unlike legacy cities, Qiddiya is being built on a foundation of digital and IoT infrastructure, creating a massive, interconnected network that demands a holistic, unified system for management, rather than siloed control rooms.

**Vision 2030 catalyst:** As a cornerstone of the national strategy, its success is a global demonstration of Saudi Arabia's commitment to an innovation-driven, non-oil economy, requiring world-class standards in safety, efficiency, and visitor experience, all managed from a central, intelligent brain.

The intelligent command center at Qiddiya, therefore, is not a standard control room; it is a Pioneering Cognitive Hub whose operational model—focused on hyper-personalization, security, and smart mobility—serves as a blueprint for the future of digitally integrated city management worldwide.



# Case study: Qiddiya Investment Company

KSA



## Introducing Qiddiya as a pioneering destination driving innovation, entertainment, and economic growth in Saudi Arabia

Qiddiya Investment Company, a subsidiary of the Public Investment Fund (PIF), plays a unique and exciting role in realizing the ambitions of Saudi Vision 2030. By embracing the transformative power of Play, Qiddiya opens doors to opportunities that empower communities and elevate the quality of life for all residents and visitors alike.

At the core of Qiddiya's mission is the belief in the Power of Play — a dynamic force driving sustainable development and long-term prosperity. Through innovative entertainment, sports, culture, and education, Qiddiya aims to stimulate economic growth and position the Kingdom of Saudi Arabia as a premier global tourist destination.

Qiddiya Investment Company is building a world-class destination set to attract 50 million visitors annually by 2030. The city will feature over 275 rides and attractions across 6 flags, Aquarabia and Dragon Ball, plus a speed park track hosting F1. Prince Mohammad bin Salman Stadium expects 7.6 million visitors and will host FIFA 2034. The Gaming and E-sports District offers 73,000 seats, uniting gamers. Merc AMG World of Performance spans 9 floors with 20 immersive attractions. The Performing Arts Center will host 200 indoor and outdoor shows yearly, with 2,000 seats across 3 venues. Additionally, there's an 18-hole state-of-the-art championship golf course.

Through these integrated experiences, Qiddiya is redefining entertainment and leisure while contributing significantly to the Kingdom's economic diversification and social enrichment goals under Vision 2030.<sup>16</sup>

## By harnessing the 'Power of Play', Qiddiya aims to drive economic growth and enhance the Kingdom's position as a global tourist destination, aligned to Vision 2030

Qiddiya aims to create destinations, programs, and initiatives to improve the quality of life for citizens, residents, and tourists. Aligned with Vision 2030, it focuses on offering new opportunities in entertainment, sports, culture, creativity, and employment.

### Qiddiya's overall objectives are as follows:

---

Establish Qiddiya City as the global capital of entertainment, sports & culture.

---

Contribute towards making Saudi Arabia a leading tourist hub by creating a world-class destination.

---

Empower Saudi youth to fulfill their ambitions and nurture their potential.

---

Offer exciting experiences for Saudi citizens, residents, and visitors.

---

Contribute to employment in tourism, hospitality & entertainment.





**Qiddiya has embarked on a journey to create an advanced Intelligent Command Center. The critical objectives are to:**

---

Maintain the 24x7 availability of all IT/OT/IoT systems, including key IT services, applications, and infrastructure and network, to meet increasing business demands as Qiddiya continues to expand.

---

Implement an advanced, unified IT/OT/IoT monitoring hub, referred to as the Intelligent Command Center (ICC), to proactively support Qiddiya's goals.

---

Establish observability across applications, databases, messaging components, middleware, virtual systems, cloud resources, and infrastructure elements including servers, network components, and any other IT/OT/IoT element within the QIC technology stack through the ICC.

---

Achieve end-to-end visibility, optimal performance, issue resolution, customer experience and improved efficiency across Qiddiya's IT/OT/IoT landscape for seamless operations and exceptional service delivery.



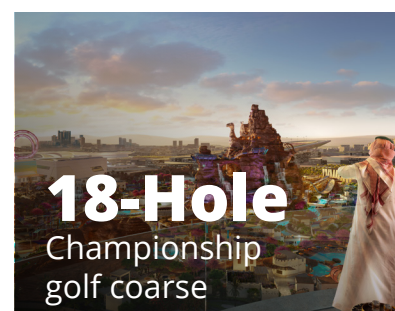
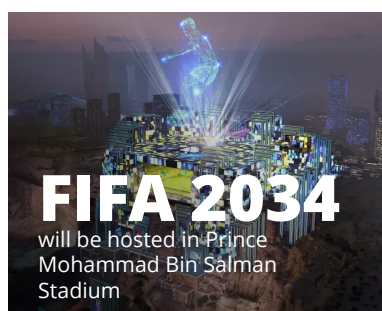
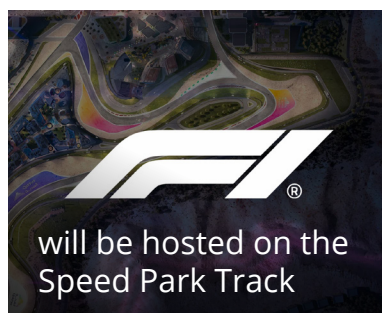
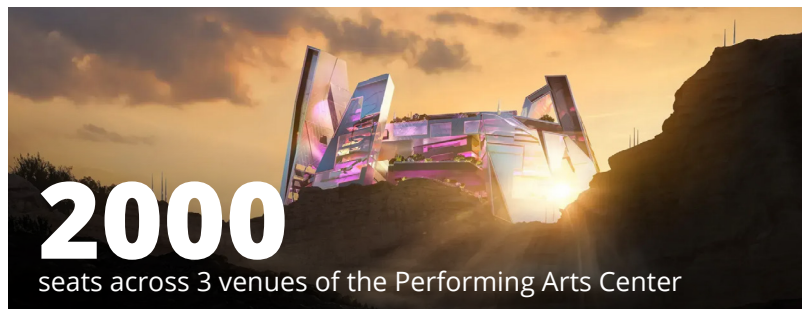


## Setting the context for the Intelligent Command Center from risk mitigation to empowered enablement

The design of the Intelligent Command Center was thoughtfully aligned with Qiddiya's development phase at the time, allowing for a comprehensive evaluation of multiple potential solutions. Each option brought its own unique considerations and challenges, which were carefully analyzed and addressed through a systematic approach.

This ensured that the final design was well-suited to meet the organization's current needs while remaining adaptable for future growth.

### A world-class entertainment destination set to transform Saudi Arabia by 2030<sup>16</sup>





**Without a centralized and seamless observability solution:**

---

Operational disruptions multiply, affecting key attractions and essential services

---

Lack of real-time visibility makes it difficult to make strategic decisions

---

Exposure to security risks compromise the safety of guests and integrity of each asset

---

**To mitigate the risks of lack of monitoring and ensure the efficient operation of Qiddiya's ecosystem, the Intelligent Command Center will act as the central observability hub for:**

---

End to end visibility and proactive incident detection

---

Operational coordination and rapid response

---

IT resilience, robustness and security

---

Improving customer experience



## Collaborating closely with Qiddiya, Deloitte's structured approach guided the successful implementation of the Intelligent Command Center, ensuring alignment with strategic goals and operational excellence

Deloitte's approach to developing Qiddiya's Intelligent Command Center was founded on a collaborative and structured methodology designed to deliver a comprehensive, future-ready solution aligned with Qiddiya's strategic ambitions.

### Vision

Central to Deloitte's approach was the principle of co-creation, working closely with Qiddiya's leadership and stakeholders to jointly define a clear and compelling vision for the Intelligent Command Center. This collaborative process ensured that the solution was not only innovative but also deeply aligned with the unique context and strategic objectives of Qiddiya's development. The vision shaped the blueprint of the architecture, providing a clear framework to deliver a flexible, scalable, and future-ready Command Center aligned with Qiddiya's ambitions.

### Blueprint

Following the establishment of the vision, Deloitte focused on developing a detailed blueprint that outlined the functional and technical requirements of the Command Center. This blueprint served as a foundational guide, capturing the key capabilities, processes, and interactions necessary to support effective command and control operations.

### Governance and operating model

Building on this, Deloitte designed a governance and operating model to ensure clear accountability, decision-making structures, and operational efficiency. This model defined roles, responsibilities, and workflows, enabling seamless coordination across various teams and stakeholders involved in the Command Center's operation.

### Technology architecture

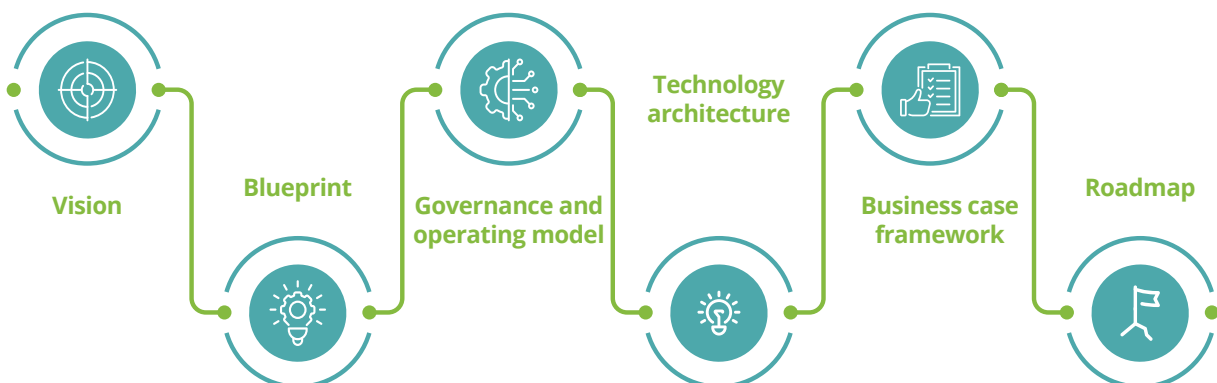
In parallel, Deloitte developed a scalable and flexible technology architecture tailored to Qiddiya's needs. This architecture integrated advanced technologies and systems to enable real-time data collection, analysis, and response capabilities, ensuring the Command Center could effectively manage complex and dynamic environments.

### Business case framework

To support the technology architecture, Deloitte developed a business case framework which was designed to align strategic objectives with financial and operational considerations, providing a clear rationale for investment. It enabled Qiddiya to evaluate potential benefits, costs, and risks systematically, ensuring informed decision-making and maximizing value realization throughout the project lifecycle.

### Roadmap

Finally, Deloitte crafted a detailed roadmap to guide the phased implementation of the Command Center, balancing immediate priorities with long-term goals. This roadmap provided a clear timeline, milestones, and resource requirements to ensure successful delivery and sustainable operation.



# Defining the guiding principles that shaped Deloitte's approach, ensuring a consistent, effective, and future-ready Intelligent Command Center for Qiddiya

Observability formed the foundation of success, ensuring that every element of the Intelligent Command Center adhered to core principles that foster Qiddiya's business growth, cost efficiency, and governance while transforming data into actionable intelligence.

## Key guiding principles included

---

### Proactivity through automation + AI

Embedding AI and other sources of automation, combined with the power of observability, will help the ICC to deliver a proactive approach in every step

---

### Scalability

Observability is providing comprehensive view of Corporate, assets and with implied standards for onboarding ensures smooth horizontal scalability

---

### Technology platform centralization

Observability enables a 360-degree knowledge of operations through a centralized platform that extracts business and tech intelligence, breaking the silos

---

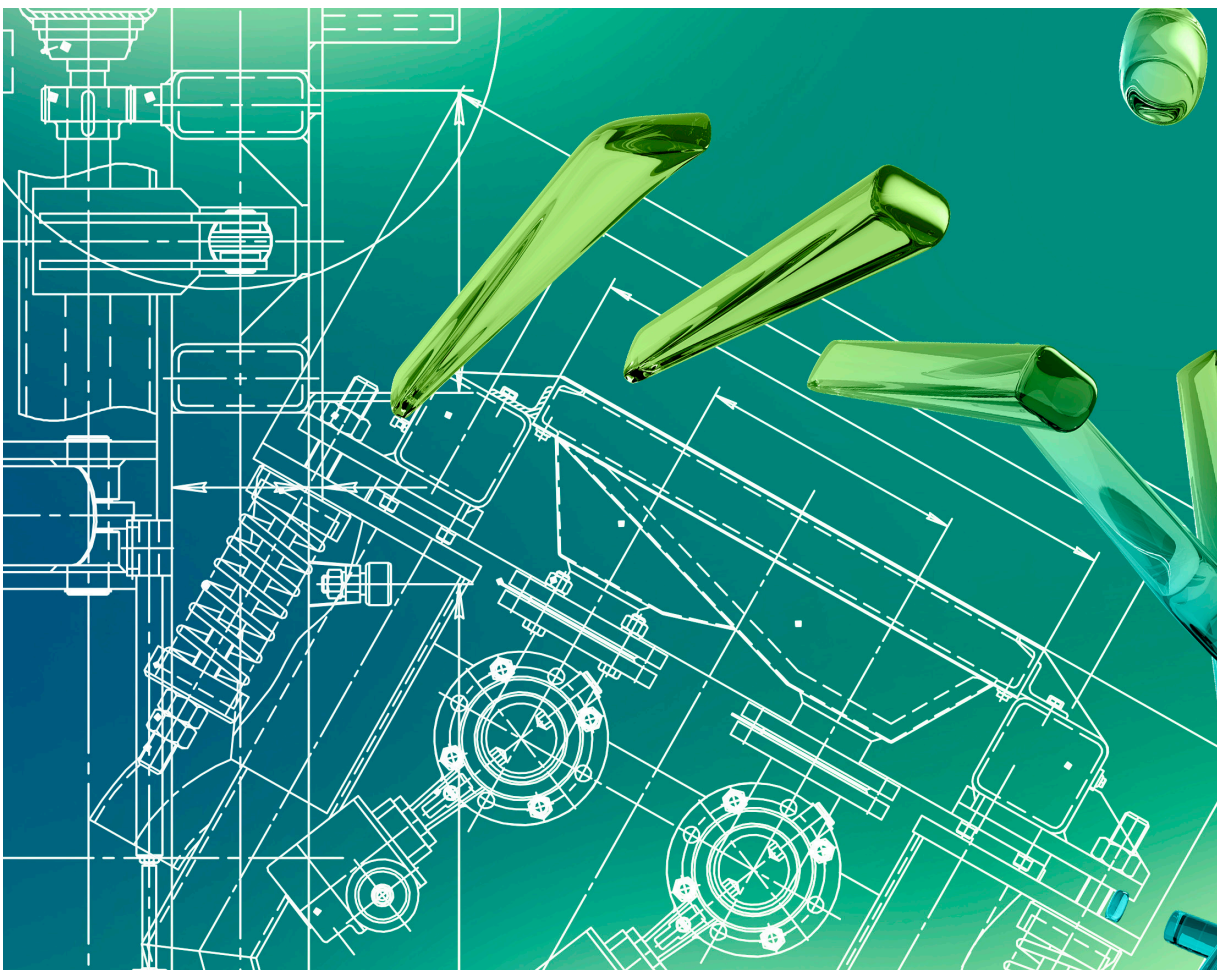
### Identify critical elements going live

Recognising the key systems and processes that must be fully operational at launch to ensure a smooth, risk-free transition and effective operation from day one.



## Developing the blueprint to provide a clear and comprehensive framework for the Intelligent Command Center's design and implementation

The blueprint for Qiddiya's Intelligent Command Center was developed through a thorough and detailed process aimed at aligning and validating key design aspects critical to the project's success. This deep dive ensured that every element of the blueprint reflects both Qiddiya's current operational requirements and its future growth ambitions. By carefully examining and confirming these design components, the blueprint provides a clear and coherent foundation that guides the development of the Command Center's architecture.



This approach guarantees that the solution remains adaptable, scalable, and fully consistent with Qiddiya's evolving needs.

### Critical success factor benchmarks

**Which Cloud Service Providers (CSPs) are the best fit for hosting the Intelligent Command Center?**

Analysis within the regional context of Qiddiya, for the CSP providers so that these are aligned within the present and future Qiddiya's needs.

### ICC suitability placement

**Which applications are prepared to be observed by the ICC?**

Internal Analysis of the applications and solutions to evaluate the suitability of these being observed in the Intelligent Command Center.

### Security monitoring

**What are the key security monitoring considerations to ensure comprehensive observability for the ICC?**

Existing IT security departments for both SEVEN and Qiddiya, it's necessary to create an aggregated view of current monitoring services, with value-added elements.

### Architecture & integration

**How should the ICC IT stack be architected and integrated with Qiddiya's ecosystem?**

Foundations for the future architecture and integrations of the ICC.

# By combining Deloitte's Strategy and Qiddiya's input, the architecture was developed to allow the ICC to fulfil the vision and goals of the journey to Enterprise Observability

## Technical requirements

The three core principles defined in the North Star Vision serve as fundamental design tenets for the Blueprint of Architecture, guiding the overall approach and framework. These principles have further evolved to inform the selection of tools from a technical perspective, ensuring alignment with the intended design.

### Cloud & SAAS first

Technologies selected should:

1. Simplify Operations: reduce infrastructure operational overhead focusing on core observability tasks providing a single pane of glass
2. Fit for thinnest viable platform (TVP): Quick addition of new features to evolve observability framework efficiently (prioritising SaaS)

### Easy connectivity

The selected tools should also:

1. Facilitate the management of networks since ecosystems contains network segments that must be managed properly
2. Foster integration with API's and connectivity standards across domains

### Easy growth (scalability)

The tools selected ensure:

- Elasticity and scalability to instantly increase/decrease the number of managed assets/applications
- Interoperability & Integration: Simplicity in adding new environments and technologies as sources
- Role-based access: Give each Team/Group specific and fine-grained access only for owned resources



## Governance requirements

Two supplementary principles have been carefully considered during the tool selection process to guarantee full compliance with the governance and legal requirements specific to the Intelligent Command Center.

### Compliance with local regulations

Technologies selected should:

1. Comply with local regulations concerning data security, residency and ensuring that all operations align with legal and industry standards
2. Incorporates high availability and disaster recovery mechanisms

### Fitness for role-based governance

Technologies selected should:

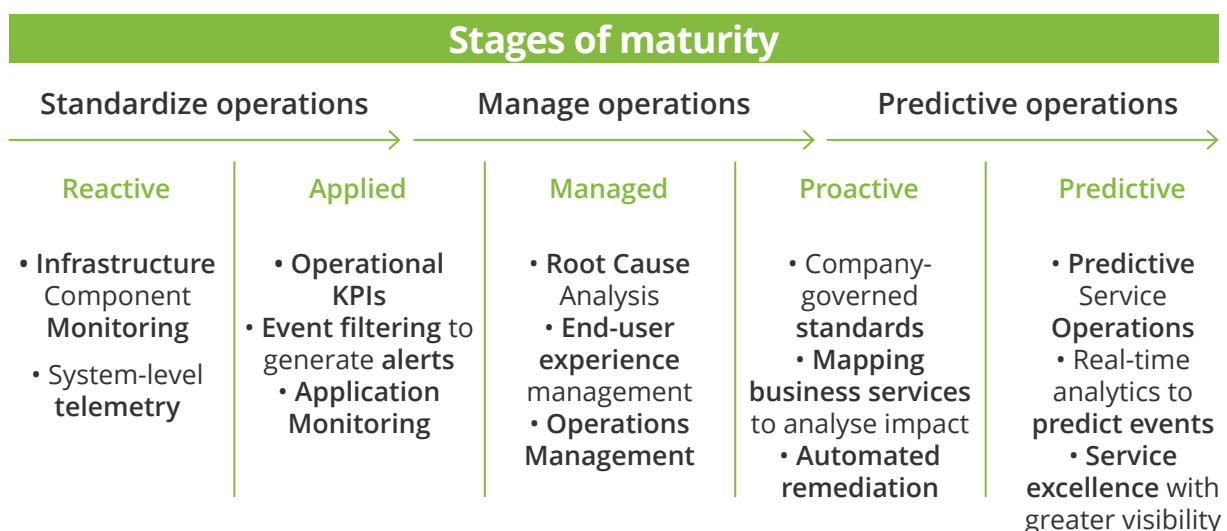
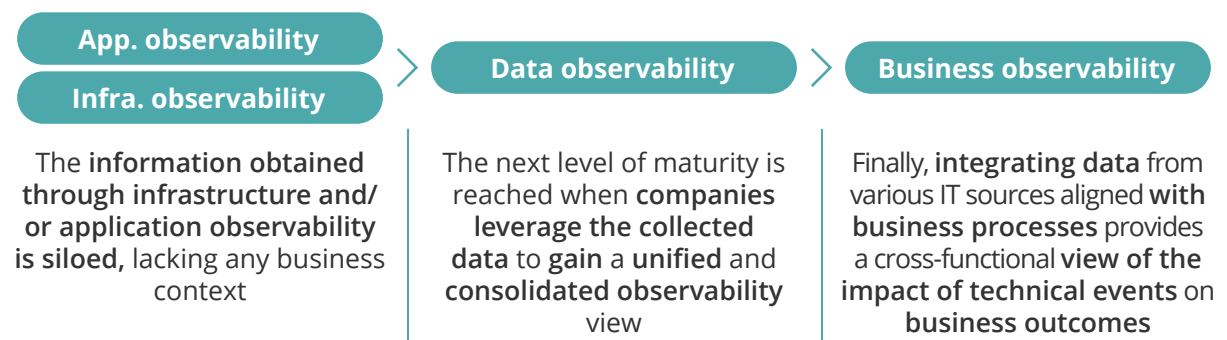
1. Ensure compliance and control through predefined policies, guardrails, and governance procedures, streamlining security and consumption management
2. Maintain financial predictability with a structured cost model, balancing baseline commitments



# The journey to End-to-End Observability was shaped through best practices to ensure comprehensive visibility and actionable insights across the ICC

Enterprise Observability builds on traditional infrastructure and application observability by bringing together data from across the entire organization. Instead of just monitoring systems or software, it connects information from IT, business processes, and customer interactions to provide a complete view of how everything works together.

This unified approach helped Qiddiya team understand how their technology affects business outcomes, allowing them to spot problems early, improve processes, and make better decisions. By turning data into clear insights, Enterprise Observability helps businesses work more efficiently and create greater value.



## The business case framework was developed to clearly demonstrate the value and impact of the ICC, supporting informed decision-making and strategic investment

Calculating the costs of the Intelligent Command Center requires a comprehensive approach that considers multiple financial factors.

**Firstly**, implementation costs must be considered; these include all expenses related to the design, development, procurement, and deployment of the Command Center's infrastructure, technology, and services. This phase often involves significant upfront investment in hardware, software, integration, and training.

**Secondly**, operating costs need to be factored in. These are the ongoing expenses required to maintain and run the ICC effectively, such as staffing, system maintenance, software licenses, utilities, and continuous support. Operating costs also cover updates and upgrades necessary to keep the Command Center aligned with evolving business needs and technological advancements.

**Finally**, it is essential to evaluate the efficiencies and cost savings generated by the ICC. By centralizing monitoring, automating processes, and enabling proactive management, the ICC can reduce downtime, optimize resource utilization, and improve response times. These efficiencies translate into tangible cost reductions and operational improvements, which should be factored into the overall cost calculation to provide a balanced view of the ICC's financial impact.

By considering implementation costs, operating costs, and the cost efficiencies gained, organizations can develop a clear and accurate business case that reflects the true value and return on investment of the Intelligent Command Center.



### ICC implementation costs

Initial costs associated with setting up the ICC, including:

- Design and planning of the ICC
- Implementation of processes, tools, and platforms
- Investment in initial infrastructure and technology
- Training and onboarding of teams

### ICC operation costs

Ongoing costs to sustain ICC operations, including:

- Cloud infrastructure to support the ICC
- Tools & services for observability platform, OS and DB licenses, etc.
- ICC Control room setup and maintenance
- In-house Personnel and 3rd party support for ICC operations

### Efficiencies driven by the ICC

Savings generated by the ICC, channeled by the OCoE helping to reduce the total cost:

- Improve Operational efficiency through automation
- Reduce downtime and service outages
- MTTR (Mean Time To Repair/Resolve) optimized by Root Cause Analysis

$$\text{Total cost of ICC} = \text{Implementation costs} + \text{Operation costs} - \text{Efficiencies driven by the ICC}$$



## Building on the business case framework, the implementation roadmap goals were defined to guide the phased delivery of the ICC, ensuring timely achievement of milestones and alignment with strategic objectives

The ICC implementation roadmap is designed to align with Qiddiya's strategic needs by providing a clear and organized plan for rolling out the Command Center's capabilities and technologies. Based on the vision, blueprint, and governance model, the roadmap ensures that each step builds on the last, supporting a smooth and effective deployment.

It focuses on establishing key foundations early, while allowing the ICC to grow and adapt over time. This approach also supports the gradual improvement of observability, moving from basic monitoring to full, end-to-end visibility and insights.



The goals of the roadmap are to guide the phased delivery of the ICC, ensure timely achievement of milestones, support scalability, and drive the maturity of observability, all while maintaining alignment with the overall strategic framework.

---

### Establish a phased and scalable implementation

The roadmap must enable a phased deployment of ICC functions, ensuring their progressive scalability.

---

### Define a technology deployment strategy

The roadmap must outline when ICC tools will be implemented, ensuring timely setup, integration, and alignment with overall observability and cybersecurity objectives.

---

### Enable the capabilities for asset launch

The roadmap must equip the ICC with the necessary functional capabilities to observe initial live assets (SEVEN, Six Flags, and Aquarabia) while enabling a scalable observability maturity.

---

### Drive the IT operating model transformation

The roadmap must support the evolution of Qiddiya's IT operating model, ensuring governance, processes, and capabilities align with the ICC's future-state vision.

---

### Structure the phased integration of applications

The roadmap must prioritize application onboarding in waves, ensuring a structured and efficient integration process based on criticality, technical dependencies, and observability maturity.

---

### Support the revaluation of the multicloud strategy

The roadmap must incorporate milestones to assess the feasibility of a multicloud approach, ensuring adaptability, resilience, and strategic alignment with evolving cloud capabilities.

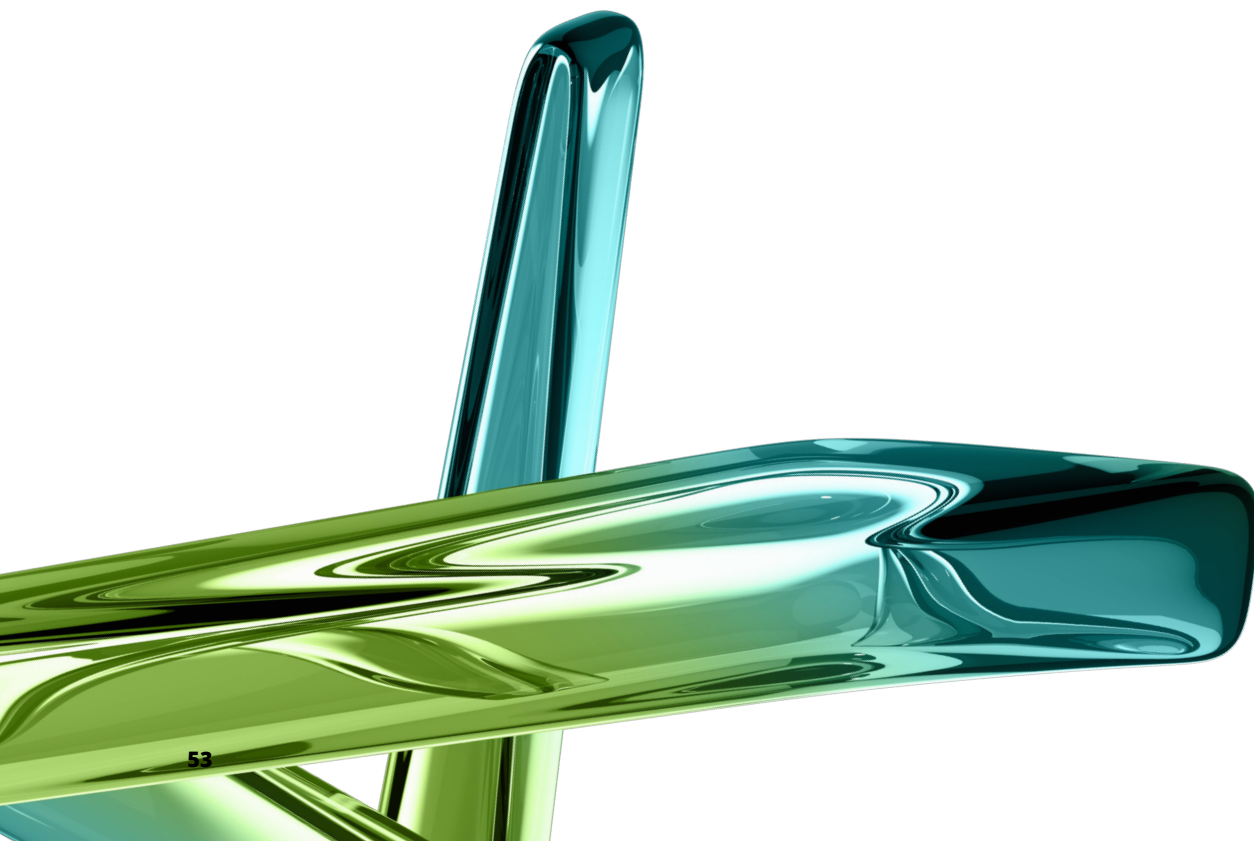


## Defining clear phases within the implementation roadmap to structure the ICC delivery, ensuring focused progress and successful realization of value at each stage

The implementation roadmap is organized into distinct, well-defined phases that provide a clear framework for the step-by-step rollout of the Intelligent Command Center. Each phase is carefully planned with specific milestones and priorities to ensure that progress is measurable and aligned with the overall objectives.

This phased approach allows for focused delivery, enabling the team to concentrate on critical tasks and capabilities at each stage before moving on to the next. By breaking the implementation into manageable segments, risks are minimized, and adjustments can be made based on learnings and feedback.

Additionally, each phase is designed to deliver tangible observability outcomes, progressively enhancing the ICC's ability to monitor, analyze, and respond to data across the organization. This ensures that observability maturity grows steadily, supporting better decision-making and operational efficiency as the Command Center evolves.



Overall, structuring the roadmap into clear phases provides a disciplined and transparent path to successfully realize the ICC's full potential.

---

## Discovery

Gathers key information, assesses existing systems, and defines the ICC foundation to ensure alignment with Qiddiya's needs

- Identify infrastructure, applications, and security components
- Define governance, processes, and observability strategies
- Assess monitoring and security capabilities

---

## Implementation

Deploys and integrates the ICC platform, establishing observability, security, and automation capabilities

- Configure monitoring, security, and automation tools
- Integrate observability and security solutions

---

## Hypercare

Monitors and fine-tunes operations to ensure a stable transition to BAU

- Perform deployment testing and validation
- Train teams for ICC operations
- Onboarding priority elements
- Launch of ICC initial operations

---

## Business as usual

Ensures continuous monitoring, optimization, and operational excellence

- Normal operation of operating model functions
- Capability scaling
- Maintain and enhance ICC platform





## Opportunities arising from the successful implementation of the Intelligent Command Center to deliver lasting value and impact

Qiddiya, is poised to become a global destination for entertainment, sports, and culture. Managing such a diverse and dynamic ecosystem requires exceptional operational intelligence. The ICC can serve as a critical enabler for Qiddiya's ambitious goals in the following ways:

**Living innovation window:** continuously evolving by embracing emerging technologies that will shape the city's future. Through the integration of AI-driven predictive analytics, digital twins, augmented reality (AR) for immersive visitor engagement, and advanced customer sentiment analysis, the ICC will enable personalized and anticipatory experiences for every guest and resident. These innovations will not only enhance operational efficiency but also transform how people interact with the city.

**Integrated security operations:** ICC brings physical security and IT security into a single command view, offering coordinated threat detection, response, and risk mitigation.

**Smart city enablement:** Qiddiya is being built as a next-generation smart city. ICC functions as the digital brain, connecting IoT systems, environmental monitoring, traffic control, and citizen services in one intelligent platform.

**Sustainable observability:** With a strong environmental agenda, Qiddiya can use the ICC to track energy consumption, emissions, and environmental impact in real-time, enabling smarter, greener operations.

By deploying an ICC, Qiddiya will gain a foundational system for performance, resilience, and safety—helping it meet international standards and offer world-class experiences.



## What success looks like

**A resilient and reliable tech platform prepared to scale both capabilities and the operating model of the Intelligent Command Center**

01

**An Intelligent Command Center operating model enhanced by technological onboarding**

02

**High availability of services, uninterrupted experiences of users powered by proactive monitoring, prompt support when and where needed**

03



## Conclusion

The Intelligent Command Center (ICC) is a strategic imperative for organisations navigating digital complexity, operational risk, and service expectations. It replaces reactive, fragmented operations with a cohesive, intelligent, and automated system of control. For giga-projects like Qiddiya, the ICC is more than an operational tool—it is a digital command nerve center that ensures reliability, agility, and leadership in a highly competitive and connected world.

Deloitte is committed to supporting Qiddiya in achieving its ambitious vision under Saudi Arabia's Vision 2030. By leveraging cutting-edge technology and strategic insights, Deloitte collaborates closely with Qiddiya to implement ICCs that drive operational excellence and innovation. This partnership exemplifies Deloitte's dedication to empowering organisations to lead in the digital age.

“Our collaboration with Qiddiya is a testament to our commitment to harnessing technology to transform operational strategies and achieve visionary goals. Through the integration of ICCs, we are not just enhancing operational capabilities; we are redefining the future of strategic management and leadership.”

Tomas Izquierdo - Senior Manager,  
Deloitte Middle East

## Authors and Contributors

### Authors



**Umashanker Achyutuni**  
Executive Director  
Corporate IT Operations,  
Qiddiya



**Tomas Izquierdo**  
Senior Manager  
Deloitte Middle East



**Hema Sethuraman**  
Manager  
Deloitte Middle East

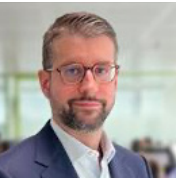
### Contributors



**Bala Sundarababu**  
Partner  
Deloitte Middle East



**Rodrigo Moreno Carton**  
Partner  
Deloitte Spain



**Hugo Izard Garcia**  
Partner  
Deloitte Spain



**Joao Ferreira Nunes**  
Partner  
Deloitte Portugal



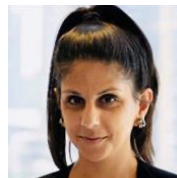
**Inna Kataeva**  
Senior Manager  
Deloitte Middle East



**Alvaro Martin del Valle**  
Senior Manager  
Deloitte Spain



**Miguel Olias** Senior  
Senior Manager  
Deloitte Spain



**Salimah Esmail**  
Senior Manager  
Deloitte Middle East



**Abubaker Ahmed**  
Senior Consultant  
Deloitte Middle East



**Nada Alrzni**  
Senior Consultant  
Deloitte Middle East



## References

1. [Security Magazine](#)
2. Gartner's Hype Cycle for AI in IT Operations
3. Gartner's Hype Cycle for AI
4. [Forbes 2025](#)
5. 18<sup>th</sup> Edition of 2025 tech trends report by FTSG
6. Science Direct 2025
7. The state of observability report 2024 – Dynatrace
8. [IBM Cost of a Data Breach Report 2023](#)
9. [IBM Cost of a Data Breach Report 2025](#)
10. 18<sup>th</sup> Edition of 2025 tech trends report by FTSG
11. Databricks
12. Nervespark.com
13. [Convergint](#)
14. [KFSHRC](#)
15. [viact.ai](#)
16. [www.Qiddiya.com](#)

## Glossary of terms

### Artificial Intelligence (AI)

Technology that enables machines to perform tasks that typically require human intelligence, such as learning, reasoning, and decision-making. In ICCs, AI drives automation, predictive analytics, and enhanced decision-making.

### Intelligent Command Center (ICC)

A centralised, adaptive platform integrating real-time observability, AI-driven automation, and coordination across IT, OT, and security environments to manage complex operations, security, and performance in organisations.

### Operational Technology (OT)

Hardware and software that detects or causes changes through direct monitoring and control of physical devices, processes, and events in an organisation.

### Information Technology (IT)

The use of computers, networking, and other physical devices to create, process, store, secure, and exchange electronic data.

### Real-time Observability

The continuous monitoring and visibility of all digital assets, systems, and services as they operate, enabling immediate detection of anomalies or issues.

### AI-Driven Automation

The use of AI to automate workflows and operational processes, reducing manual intervention and increasing efficiency.

### Predictive Analytics

AI-powered analysis that anticipates potential threats or operational challenges before they occur, allowing proactive responses.

### Centralised Coordination

The unified management and orchestration of operations, security, and incident response across multiple teams and systems from a single platform.

### Cybersecurity Intelligence

Information and insights related to cyber threats, vulnerabilities, and risks used to strengthen an organisation's security posture and response capabilities.

### Unified Monitoring

The consolidation of monitoring activities across infrastructure, applications, networks, physical assets, and services into a single platform.

### Automated Workflows

Predefined, AI-enabled processes that handle incident detection, remediation, escalation, and other operational tasks without manual input.

### Fragmented Visibility

A challenge where data and monitoring are scattered across multiple tools, teams, and environments, leading to incomplete situational awareness.

### Operational Agility

The ability of an organisation's teams to respond quickly, collaborate effectively, and adapt to changing conditions.

### Cyber-Resilience

The capacity to anticipate, withstand, recover from, and adapt to cyber attacks and threats.

### Modular Architecture

A design principle where the system is composed of interchangeable components that can be independently developed, replaced, or upgraded.

### Technology-Agnostic

The capability of a system to integrate seamlessly with a variety of legacy and modern technologies without dependency on specific platforms.

### Smart City Enablement

The use of digital technologies, including IoT and AI, to manage city infrastructure and services efficiently and sustainably.

### Giga-Projects

Large-scale, complex projects with significant economic, social, or infrastructural impact, such as Qiddiya under Saudi Arabia's Vision 2030.

### Qiddiya

A flagship giga-project in Saudi Arabia aimed at becoming a global destination for entertainment, sports, and culture, requiring advanced operational intelligence.

### Vision 2030 (Saudi Arabia)

A strategic framework aimed at economic diversification and development in Saudi Arabia, supporting projects like Qiddiya.

### Incident Resolution Time

The duration taken to detect, respond to, and resolve operational or security incidents.

### Crowd Analytics

The use of data and AI to monitor, predict, and manage the movement and behaviour of crowds, especially during large public events.

### Environmental Monitoring

Tracking and analysing environmental factors such as energy consumption and emissions to support sustainability goals.

### Compliance Visibility

The ability to monitor and ensure adherence to regulatory and governance requirements within operational processes.





This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication.

Deloitte & Touche (M.E.) (DME) is an affiliated sublicensed partnership of Deloitte NSE LLP with no legal ownership to DTTL. Deloitte North South Europe LLP (NSE) is a licensed member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of DTTL, its global network of member firms, and their related entities.

DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL, NSE and DME do not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories, serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 457,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

DME would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. DME accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

DME is a leading professional services organization established in the Middle East region with uninterrupted presence since 1926. DME's presence in the Middle East region is established through its affiliated independent legal entities, which are licensed to operate and to provide services under the applicable laws and regulations of the relevant country. DME's affiliates and related entities cannot oblige each other and/or DME, and when providing services, each affiliate and related entity engages directly and independently with its own clients and shall only be liable for its own acts or omissions and not those of any other affiliate.

DME provides services through 23 offices across 15 countries with more than 7,000 partners, directors and staff. It has also received numerous awards in the last few years such as the 2023 & 2022 Great Place to Work® in the UAE, the 2023 Great Place to Work® in the KSA, and the Middle East Tax Firm of the year.

**© 2025 Deloitte & Touche (M.E.). All rights reserved.**