

ADVANCING READINESS STRENGTHENING RESILIENCE

Building the Middle East's next standard for emergency preparedness and response - an all-hazards agenda spanning pandemics, climate extremes, mass gatherings, cyber disruption and critical infrastructure continuity

Dr. Paul Setlak, PharmD, MBA

Founder & Chief Executive Officer | Al-Ghaf Dynamics

Benjamin Vile

Chief of Security and Response Operations

June 2026



Across the Middle East, governments and institutions have built substantial emergency plans, modern infrastructure and deep operational experience. The next opportunity is to convert that strong foundation into tested, funded and interoperable capabilities that continue performing when several systems are under pressure at once.

“Preparedness is the demonstrated ability to detect early, decide quickly, coordinate across boundaries, sustain essential services and recover with discipline.”

After years working across clinical care, public health, emergency response, healthcare strategy and operational delivery, I have reached a simple conclusion: the greatest readiness gains come from removing ambiguity at the exact moment decisions must be made. Authority should be unmistakable. Activation thresholds should be objective. Data should converge into one operating picture. Public and private partners should work to a shared rhythm. Supplies should be managed against known burn rates. Communications should move at operational speed. Exercises should translate lessons into funded, verified action.

The Middle East is especially well positioned to lead this agenda. Its major aviation and maritime hubs connect continents. Energy, water, food, telecommunications and logistics systems are tightly interdependent. Cities host large, mobile and multilingual populations, while religious, sporting, cultural and commercial events bring millions of people together. These strengths coexist with a demanding risk environment that includes extreme heat, flash flooding, sand and dust storms, infectious disease threats, water stress, conflict and displacement in parts of the wider region, and rapid digitalization of critical infrastructure. The same connectivity that creates exposure also creates a powerful platform for coordinated, technology-enabled resilience.

Recent assessments from the World Health Organization, the United Nations Office for Disaster Risk Reduction and the World Meteorological Organization underline a strategic opportunity: because risk is interconnected, preparedness investments can strengthen multiple systems at once. A respiratory outbreak can affect workforce availability and supply chains. A heatwave can stress electricity, water, occupational health and hospital capacity. A flood can affect roads, ambulance access, power, telecommunications, water safety and pharmaceutical distribution. A cyberattack can disrupt clinical systems during a mass-casualty incident. The answer is not to plan for each hazard in isolation, but to build common capabilities that absorb and coordinate across cascading effects.

The next step is therefore not another plan. It is a disciplined progression from plans to performance: an operating system that produces timely decisions, coordinated action and measurable continuity under stress.

A connected view of the Middle East risk landscape

An all-hazards approach is sometimes misunderstood as a generic plan that treats every emergency the same. That is not the objective. The objective is to build common capabilities that work across emergencies, then add hazard-specific procedures where the science and operations differ. Command, coordination, logistics, public information, workforce management, resource tracking and continuity should be common. Isolation protocols, decontamination, radiation monitoring, crowd-flow management and vector control require specific annexes and trained teams.

For leaders in the Middle East, a credible, future-ready risk architecture should address the following threat families and the cascades they can generate:

- **Pandemics, epidemics and emerging infections.** Respiratory pathogens, zoonotic spillover, food- and waterborne disease, vector-borne infections, antimicrobial resistance and imported cases can move quickly through highly connected populations. The core planning question is not which pathogen comes next, but whether surveillance, laboratories, hospitals, supply chains, employers and public communication can scale together.
- **Extreme heat and occupational exposure.** Heat affects cardiovascular, renal and respiratory health; increases ambulance demand; reduces outdoor labor productivity; stresses electricity and water systems; and threatens medication, laboratory reagent and vaccine storage. Heat planning must link health alerts to employers, schools, municipalities, utilities, event organizers and community services.
- **Flash floods, severe storms and coastal hazards.** In arid environments, intense rainfall can overwhelm drainage, cut road access, contaminate water, flood healthcare facilities and disrupt power and telecommunications. The most important controls often sit outside the health sector.
- **Sand, dust and deteriorating air quality.** Dust events can increase respiratory and cardiac presentations, disrupt aviation and transport, reduce visibility, affect equipment and compound risk for outdoor workers and vulnerable patients.
- **Water scarcity, drought and food-system disruption.** Water stress affects hygiene, infection prevention, agriculture, food prices, population movement and continuity of care. Desalination, energy and water systems must be treated as one critical dependency rather than separate sectors.
- **Earthquakes and geophysical hazards.** Several parts of the wider region face significant seismic risk. Preparedness must cover structural safety, mass casualty management, hospital evacuation, search and rescue interfaces, shelter, family reunification and prolonged disruption of essential services.
- **Industrial, chemical and hazardous-material incidents.** Petrochemical facilities, ports, transport corridors, laboratories and industrial zones create legitimate high-consequence scenarios. Hospitals must be ready to receive contaminated patients without becoming contaminated themselves.
- **Radiological and nuclear emergencies.** The growth of nuclear technology and the movement of radioactive sources require clear interfaces among regulators, civil defense, health authorities, hospitals, radiation protection teams and public warning systems.
- **Conflict, insecurity and humanitarian emergencies.** Mass casualty incidents, displacement, damaged infrastructure, interrupted supply chains and attacks on healthcare can create long-duration crises in which continuity, protection and recovery must be managed together.

- **Cyber and technology disruption.** Ransomware, cloud outages, data compromise and telecommunications failure can interrupt clinical care, dispatch, laboratory reporting, public warning and supply-chain visibility. Cyber response and emergency management can no longer be separate disciplines.
- **Mass gatherings and high-volume mobility.** Saudi Arabia's extensive operational experience in Hajj and Umrah, together with the region's major sporting events, exhibitions, festivals and international conferences, provides a distinctive platform for advancing integrated planning for heat, crowd safety, infectious disease, emergency medical services, multilingual communication and rapid referral.
- **Critical infrastructure and supply-chain interruption.** Healthcare depends on electricity, fuel, water, oxygen, transport, digital platforms, cold chain, imported medicines and specialized vendors. A system is only as resilient as the weakest unrecognized dependency.

A PRACTICAL MODEL FOR AN ALL-HAZARDS SYSTEM

Common capabilities for every emergency: governance, risk intelligence, incident management, logistics, public communication, workforce, continuity, finance and recovery.

Hazard-specific capabilities where operations differ: infection prevention, laboratory surge, decontamination, radiation monitoring, crowd management, vector control, sheltering and evacuation.

A shared assurance process that proves both layers work together under realistic conditions.

Where leaders can unlock the greatest readiness gains

Many organizations already have substantial plans, experienced personnel and modern facilities. The greatest near-term gains sit at the interfaces between departments, sectors and jurisdictions. The following opportunities deserve direct executive attention.

Make emergency authority immediately executable

An executable plan specifies who can declare an emergency, activate an operations center, release emergency funds, requisition private assets, suspend routine rules and authorize public messages. In a fast-moving event, clear decision rights protect valuable time. They should be pre-delegated, legally reviewed and exercised.

Use clear thresholds to support early action

Clear triggers combine hazard severity, rate of change, geographic spread, healthcare pressure, critical-infrastructure impact and public concern. Leaders also need permission to activate early when evidence is incomplete but the downside of delay is high.

Coordinate around consequences, not institutional boundaries

Health, police, civil defense, municipalities, regulators, utilities, airports, ports and private providers may each have a valid plan. High-performing systems also share terminology, escalation levels, reporting cycles, liaison arrangements and resource-request procedures so coordination accelerates as demand rises.

Build surge capacity as a complete operating system

Usable surge capacity is a complete care pathway. Every additional bed requires staff, oxygen, medications, equipment, diagnostics, waste management, infection prevention, transport, food, security and information systems. Capacity should therefore be measured as a functioning system, not as space alone.

Manage stockpiles for endurance and replenishment

Operational stockpile management connects inventory to consumption rates, shelf-life control, allocation rules, alternate suppliers, transport arrangements and replenishment contracts. The key measure is endurance: how long can the organization sustain a defined level of demand?

Use communication as an operational capability

Risk communication is an intervention. It should tell people what has happened, what is known, what is uncertain, what actions to take, where to obtain help and when the next update will come. In a multilingual region, communication plans must cover language, accessibility, trusted messengers, rumor management and feedback from communities.

Prove digital resilience through restoration and downtime operations

Digital resilience is demonstrated when backups, alternate sites and redundant links can be restored, connected and used under realistic load. Every critical digital process needs a tested downtime procedure, an out-of-band communication method and a clear recovery sequence.

Turn every exercise into funded, verified improvement

A high-value after-action review identifies capability priorities, assigns owners, secures funding and closes actions by a fixed date. Preparedness improves when lessons become verified corrective action and are retested.

Design recovery from the start

Recovery begins with decisions made in the first days. Those decisions shape service restoration, workforce retention, public trust and long-term resilience. Recovery priorities, financing, data needs and governance should be designed before the emergency and activated while response operations are still strong.

A connected readiness architecture for the Middle East

The strongest regional model combines aligned national standards with empowered local execution. The UAE's federal and emirate-level operating environment provides a strong platform for shared doctrine, interoperable systems and locally responsive action, while the wider region offers multiple models that can be adapted to national context. The following capabilities form a practical readiness architecture for governments, health systems, infrastructure operators, major employers and event organizers.

- 01 **Accountable governance and emergency authority**
Every system needs an executive owner, a lead operational authority and a governance structure that can move from routine monitoring to crisis decision-making without confusion. Legal powers, emergency procurement, funding release, data sharing, private-sector requisition, mutual aid and public communication authority should be documented in advance. A small crisis policy group should handle strategic trade-offs while the incident management team directs operations. Both groups need decision logs and a defined rhythm.
- 02 **Integrated risk intelligence and early warning**
Risk intelligence should combine traditional surveillance with meteorological alerts, environmental monitoring, veterinary data, poison-center calls, emergency-department syndromes, laboratory signals, medicine demand, school or workplace absenteeism, social listening and infrastructure status. A common operating picture should show what changed, why it matters, likely scenarios, decisions required and confidence levels. Information without thresholds and decision ownership is not intelligence.
- 03 **Interoperable incident management and emergency operations centers**
Emergency operations centers should use common terminology, activation levels, functional roles, situation-report formats, resource-request processes and shift-handover standards. Liaison officers from health, civil protection, police, municipalities, utilities, transport, telecommunications and major private providers should be pre-identified. Alternate physical and virtual locations must be tested. The objective is not a room full of screens; it is a disciplined decision process.
- 04 **One Health surveillance, laboratories and diagnostic networks**
Human, animal and environmental intelligence must be connected before a zoonotic or food-system event occurs. Laboratory networks need clear referral pathways, sample transport, surge testing, quality assurance, biosafety, biosecurity, genomic sequencing and result-reporting standards. Data-sharing agreements should specify what can move, with whom, at what level of detail and under what emergency authority.
- 05 **Resilient health services and complete surge pathways**
Health systems should define which services must continue under every scenario and which can be reduced or relocated. Emergency and intensive care capacity, oxygen, dialysis, maternity, oncology, trauma, mental health, chronic disease medicines and infection prevention all require continuity plans. Public and private hospitals, ambulance providers, primary care, pharmacies and laboratories should operate within one referral and load-balancing framework.

06

Medical countermeasures, procurement and supply-chain endurance

Preparedness requires risk-based lists of medicines, vaccines, diagnostics, PPE, antidotes, consumables, oxygen components and critical spare parts. Leaders need visibility of inventory, burn rate, days of supply, shelf life, supplier concentration, transport constraints and substitution options. Framework agreements, emergency regulatory pathways, allocation principles and regional sourcing arrangements should be negotiated before demand becomes global.

07

Critical infrastructure, cyber resilience and emergency telecommunications

Each critical function should map its dependency on power, water, fuel, oxygen, mobile networks, cloud services, specialized vendors and physical access. Recovery time objectives should be linked to clinical and operational consequences. Cyber incident teams must participate in emergency exercises, and emergency managers must understand how to operate during digital downtime. Radio, satellite, secure messaging and manual fallbacks should be used, not merely stored.

08

Risk communication, community engagement and public warning

Communication should be operational from the first hour. Pre-approved message templates, spokesperson arrangements, multilingual translation, accessible formats, rumor tracking, community feedback and sector-specific guidance should be ready. Authorities should identify trusted messengers for different communities, including migrant workers, older adults, people with disabilities and remote populations. Trust is built through speed, transparency, consistency and visible correction when information changes.

09

Mass-gathering, transport and points-of-entry readiness

Airports, ports, border crossings and mass gatherings require joint risk assessment, event-based surveillance, medical-post design, heat and crowd plans, isolation and referral procedures, ambulance egress, passenger information and cross-border notification. Event organizers should operate a health security cell that connects directly to the relevant operations center and can continue surveillance after the event ends.

10

Workforce readiness, reserve capacity and responder protection

A workforce plan should identify critical roles, trained alternates, call-down procedures, credentialing, reserve pools, occupational health, PPE, vaccination, transport, accommodation, fatigue management and psychosocial support. Staff family needs matter: people are less able to report for duty when they do not know whether their children, parents or dependents are safe.

11

Business, education and community continuity

Government continuity alone is insufficient. Major employers, schools, universities, childcare providers, food distributors, logistics companies, pharmacies and small businesses influence whether society can function. Business continuity requirements should be proportionate to sector criticality, connected to public warning and included in exercises. Education continuity should cover physical safety, remote learning, school feeding, student wellbeing and family communication.

12

Exercises, assurance, recovery and institutional learning

Preparedness should be tested through a progressive program: communications checks, call-down drills, tabletops, functional exercises and full-scale exercises. Scenarios should test real interfaces, night and weekend staffing, supplier failure, misinformation and simultaneous hazards. Recovery governance, data preservation, damage assessment, financial tracking and improvement planning should be activated during the exercise rather than discussed afterward.

Building pathogen-agnostic, operationally specific pandemic readiness

The next pandemic will not arrive as a replay of COVID-19. It may have a different transmission route, severity profile, age distribution, incubation period, geographic pattern or countermeasure timeline. A credible plan therefore starts with pathogen-agnostic capabilities and then organizes operational modules around transmission: respiratory, contact, vector-borne, food- and waterborne, and zoonotic threats.

The amended International Health Regulations and the WHO Pandemic Agreement signal higher expectations for national coordination, surveillance, financing, medical countermeasures, workforce protection, supply-chain resilience and equity. The Pandemic Agreement has been adopted, while work on its Pathogen Access and Benefit-Sharing annex continues before the full agreement opens for signature and ratification. Organizations do not need to wait for the legal process to finish before strengthening practical readiness.

A pandemic plan should answer the following operational questions in plain language:

- **How will a weak signal be verified?** Define who receives alerts, how epidemiological and laboratory information is validated, when a rapid risk assessment is launched and who can escalate based on incomplete information.
- **What triggers each activation level?** Use epidemiology, severity, geographic spread, health-system pressure, critical-workforce impact, countermeasure availability and public concern. Do not rely on case counts alone.
- **How will diagnostics scale?** Specify reference laboratories, surge platforms, sample collection, transport, biosafety, quality control, genomic sequencing, data integration and prioritization when demand exceeds capacity.
- **How will essential health services continue?** Predefine service-protection priorities for emergency care, maternity, dialysis, oncology, chronic disease, immunization, mental health and medicine access. Pandemic response cannot be allowed to create avoidable mortality from every other condition.
- **Where will clinical surge come from?** Identify complete care pathways: staff, oxygen, beds, equipment, pharmacy, imaging, laboratory, infection prevention, waste, transport and referral. Define the thresholds for cohorting, alternate care sites and interfacility load balancing.

- **How will the workforce be sustained?** Plan for absenteeism, quarantine, burnout, illness, transport disruption and family responsibilities. Cross-train critical roles, create reserve pools and protect staff physically and psychologically.
- **How will public health and social measures be selected?** Use a transparent decision framework that weighs transmission, severity, feasibility, equity, economic impact and health-system capacity. Measures should have clear objectives, review dates and exit criteria.
- **How will medical countermeasures be allocated?** Establish procurement, regulatory, pharmacovigilance, cold-chain, delivery and ethical allocation processes for vaccines, medicines, diagnostics and protective equipment. Prioritization principles should be agreed before scarcity.
- **How will borders and mass gatherings be managed?** Connect points of entry and event organizers to surveillance, referral, laboratory and communication systems. Travel measures should be risk-based, time-limited and operationally feasible.
- **How will information move?** Build secure data exchange across public health, clinical care, laboratories, private providers, employers and national authorities. Provide decision-makers with a concise common operating picture rather than parallel dashboards.
- **How will the public be kept informed?** Prepare multilingual messages for the first confirmed case, community transmission, vaccine or medicine availability, service changes, isolation guidance and rumor correction. State what is unknown and when it will be updated.
- **How will the system transition to recovery?** Define criteria for de-escalation, backlog recovery, workforce restoration, long-term surveillance, financial reconciliation, evaluation and institutional learning.

A PRACTICAL PANDEMIC ACTIVATION LADDER

Watch: an external signal with plausible regional relevance. Increase monitoring, review readiness and confirm contacts, supplies and laboratory pathways.

Alert: a verified event with increased importation or local amplification risk. Launch a formal risk assessment, activate selected coordination functions and issue targeted guidance.

Partial activation: imported cases, local clusters, rising severity or measurable health-system pressure. Activate the emergency operations structure, surge surveillance, laboratories, communications and healthcare readiness.

Full activation: sustained community transmission, multi-jurisdiction impact or systemic disruption. Move to whole-of-government coordination, continuity protection, medical-countermeasure allocation and sustained public communication.

The exact thresholds should be country- and hazard-specific. The important point is that leaders agree them, rehearse them and retain authority to act early.

Integrating climate readiness with health and emergency management

Climate-related readiness is an opportunity to protect health, infrastructure and economic continuity through one coordinated operating model. Extreme heat, drought, flash flooding, severe storms and dust events can affect multiple systems at the same time. Connecting climate strategy to emergency operations, hospitals, employers and public warning enables earlier action and stronger protection during acute events.

Protecting health and continuity during extreme heat

Heat-health action plans should link meteorological thresholds to graded actions across health authorities, emergency medical services, hospitals, municipalities, schools, employers, utilities and event organizers. Actions should include occupational work-rest guidance, hydration and shaded rest, outreach to high-risk individuals, cooling locations, ambulance and emergency-department surge, medication-storage protection, power-failure contingencies and public messages in relevant languages. Plans must account for humidity and nighttime temperatures, not air temperature alone.

Strengthening readiness for flash floods and severe rainfall

Flood readiness should identify vulnerable roads, tunnels, healthcare facilities, substations, water assets, low-lying communities and supply routes. Health facilities need drainage and waterproofing checks, safe generator and fuel locations, evacuation and shelter-in-place triggers, protected medical gases and continuity for laboratories and pharmacies. Public warning should be linked to road closures, school decisions, ambulance routing, water-safety guidance and post-flood vector control.

Managing sand, dust and air-quality events proactively

Dust plans should integrate air-quality monitoring with guidance for schools, outdoor workers, sporting events, people with chronic respiratory disease, aviation and road transport. Hospitals and ambulance services should anticipate increased respiratory demand, protect filtration systems and confirm oxygen resilience. Communication should be action-oriented: who should stay indoors, which masks are useful, when outdoor activity should stop and how to seek care.

Protecting continuity and accelerating recovery in humanitarian settings

In conflict-affected and fragile settings, the most effective preparedness model protects trauma services while sustaining the wider health system. It connects trauma care with outbreak control, water and sanitation, chronic care, mental health, medicine supply, facility continuity and workforce protection. This integrated model links humanitarian response with health-system continuity and early recovery.

Practical priorities include protected referral routes; distributed stocks; mobile and modular services; secure and redundant communications; mass-casualty triage; blood, oxygen and surgical capacity; continuity for dialysis, maternity and chronic medicines; outbreak surveillance in displacement settings; vaccination and water-quality controls; family tracing and patient identification; staff evacuation and replacement; and mechanisms to document attacks on healthcare and protect neutral medical action. Recovery planning should begin while response operations are active so temporary measures create a bridge to stronger, durable services.

Mass gatherings as a platform for national readiness and innovation

Saudi Arabia's leadership in Hajj and Umrah, together with the Middle East's extensive experience in major sporting, cultural and commercial gatherings, provides a valuable platform for national capability building. These events concentrate many of the same operational requirements seen in wider emergencies: high population density, heat exposure, rapid mobility, infectious disease surveillance, crowd management, multilingual communication, transport coordination, medical surge and intense public scrutiny.

A high-performing event health security model begins months in advance with a joint risk assessment and an integrated command structure. It includes syndromic and event-based surveillance, laboratory referral, on-site triage and treatment, ambulance egress, hospital load balancing, heat and crowd thresholds, food and water safety, isolation capacity, multilingual public messages, rumor monitoring, accessibility arrangements and post-event surveillance. Suppliers, venues, transport operators, hotels, tour providers and private healthcare should be connected to the same common operating picture.

The enduring value comes after the event: transfer the tested procedures, trained personnel, dashboards, communications and after-action lessons into routine national and local emergency readiness.

Strengthening the hospital interface for CBRN and industrial readiness

Chemical, biological, radiological and nuclear specialist agencies bring essential expertise. That expertise creates the greatest value when it is tightly connected to emergency medical services, hospitals and public communication. A contaminated patient may reach a hospital before the facility receives an official alert, and evacuation decisions are safest when transport, shelter and health support are synchronized.

Preparedness should cover hazard identification, scene zoning, responder protection, decontamination, antidotes, radiation monitoring, contaminated-patient routing, hospital lockdown or controlled access, shelter-in-place and evacuation criteria, waste and evidence handling, poison-center and radiation-specialist consultation, and coordinated public warning. Exercises should begin with an ambiguous first report and test whether the receiving hospital recognizes the hazard before contamination spreads through the emergency department.

Embedding cyber resilience in patient safety and emergency command

A cyber incident can be a health emergency even when no physical infrastructure is damaged. Electronic records, medication administration, diagnostic systems, ambulance dispatch, laboratory reporting, staff communications and supply ordering may all be affected. The most dangerous scenario is a cyber failure during another emergency, when demand is already high and workarounds are under pressure.

Healthcare and emergency organizations should maintain tested downtime procedures for patient identification, medication orders, laboratory requests, imaging, bed management, referral, public reporting and mortality documentation. Backups should be restored in exercises, not merely reported as successful. Leaders should know which systems must recover first, what data can be reconciled later, how teams communicate out of band and what manual workload can be sustained for twelve, twenty-four and seventy-two hours.

Bringing the private sector into readiness from the outset

The region's emergency capacity is strengthened by a diverse network across government entities, private hospitals, pharmacies, laboratories, airlines, ports, telecommunications companies, logistics providers, hotels, universities, manufacturers, retailers and major employers. A national plan creates greater capacity when these organizations are integrated as operational partners and their dependencies are governed in advance.

Preparedness agreements should define data sharing, liaison roles, emergency procurement, mutual aid, staff credentialing, priority access, transport, warehousing, public messaging and cost recovery. Contracts with critical suppliers should contain emergency service levels, alternate routing, inventory transparency and participation in exercises. The strongest systems know and exercise with their private-sector partners before activation.

Making readiness measurable through time, endurance and closure

Preparedness dashboards often rely on self-assessed maturity scores. These are useful, and leaders gain a fuller picture when they are paired with performance measures showing how quickly the system acts, how long it can continue and whether agreed improvements are being closed. The following measures are more revealing than the number of plans on a shelf:

- **Signal-to-verification time.** How long does it take to validate an unusual event and produce an initial risk assessment?
- **Decision-to-activation time.** How long from an agreed trigger to a staffed and functioning coordination structure?

- **Time to first public message.** Can an accurate, actionable and multilingual message be issued while uncertainty remains?
- **Time to first common operating picture.** Can leaders see the same event, impacts, decisions and resource gaps within the first operational period?
- **Critical-role depth.** What proportion of essential roles have at least two trained alternates who have exercised the function?
- **Infrastructure endurance.** How many hours or days can critical services operate without grid power, normal water supply, primary telecommunications, routine fuel delivery or cloud access?
- **Clinical surge time.** How quickly can usable emergency, intensive-care or alternate-care capacity be added with staff, oxygen, medicines and diagnostics?
- **Laboratory surge and turnaround.** What testing volume can be sustained, and how rapidly do priority results reach decision-makers?
- **Supply-chain endurance.** How many days of supply exist at defined demand levels, and how concentrated are critical suppliers?
- **Workforce mobilization time.** How quickly can reserve staff be contacted, credentialed, protected, transported and deployed?
- **Essential-service continuity.** Which services continued, at what capacity and with what backlog during the exercise or event?
- **Message reach and comprehension.** Did priority populations receive, understand and act on the warning?
- **Corrective-action closure.** What proportion of after-action items were completed, tested and independently verified by the due date?
- **Recovery milestone time.** How quickly are priority services, workforce, data, finance and routine governance restored?

THE SEVEN-QUESTION LEADERSHIP READINESS CHECK

Can we detect the event early enough to matter?

Can the right person decide before the evidence is complete?

Can organizations coordinate through one operating picture?

Can we communicate clearly to every priority population?

Can health and essential services surge without abandoning routine care?

Can we sustain operations when power, data, staff or supplies are constrained?

Can we recover, close the gaps and prove that the system improved?

Exercise the interfaces that determine real-world performance

Exercises create the greatest value when they test the points where responsibility changes hands: laboratory to public health, public health to emergency management, ambulance to hospital, regulator to operator, government to private sector, operations center to spokesperson, central authority to local teams and response to recovery. A tabletop within one department is useful; a cross-system exercise reveals whether the whole operating model can perform.

A credible baseline for a major institution or jurisdiction is a progressive annual program:

- **Routine communications checks.** Test alerting systems, contact lists, radios, secure messaging and alternate channels. Rotate nights, weekends and holidays.
- **Quarterly call-down and coordination drills.** Confirm who responds, how quickly they report and whether the operations center can establish an initial common operating picture.
- **Semiannual tabletop exercises.** Use senior leaders to test policy decisions, authority, trade-offs, public communication and cross-sector dependencies.
- **Annual functional exercises.** Operate the command structure in real time with simulated data, resource requests, public messages, shift handovers and supplier participation.
- **Periodic full-scale exercises.** Deploy field teams, emergency medical services, hospitals, laboratories, decontamination, transport, shelters or event operations as relevant.
- **After-action closure.** Complete the review rapidly, assign each improvement to an accountable owner, secure resources, set a deadline and retest the correction.

The scenario should include friction: conflicting reports, an absent decision-maker, a failed supplier, a social-media rumor, a telecommunications outage, an unexpected vulnerable population and a second hazard. Emergencies do not wait for the first problem to be solved before presenting the next one.

A practical ninety-day pathway to stronger readiness

Readiness improvement can begin without waiting for a multiyear transformation program. A disciplined ninety-day cycle can establish the baseline, create executive ownership and generate momentum.

Days 0-30: establish the baseline.

1

Confirm the executive sponsor and operational lead. Select the priority all-hazards scenarios. Identify essential services and their dependencies. Review legal authority, activation thresholds, emergency finance, contact lists, mutual-aid arrangements, supply endurance and open corrective actions. Interview frontline staff, not only plan owners.

Days 31-60: translate priorities into operating procedures.

2

Update the concept of operations, activation levels, decision rights, information requirements, resource-request process, crisis communications, workforce reserve, critical-supplier arrangements and continuity procedures. Pre-draft the first-hour public messages and establish a concise readiness dashboard.

3

Days 61-90: exercise, improve and commit.

Run a functional exercise that includes executives, operations, frontline teams, private partners and communications. Complete the after-action review, assign and fund corrective actions, report the results to the board or governing authority and approve a twelve-month capability-building roadmap.

Leadership questions that build confidence and accountability

- What must still work at two hours, twenty-four hours, seventy-two hours and fourteen days?
- Who can declare an emergency, activate the operations center, release funds and authorize the first public message?
- What are the objective triggers for escalation and de-escalation?
- Which critical services have a single point of failure in people, technology, utilities or suppliers?
- What happens if the electronic health record, mobile network or primary operations center is unavailable?
- How long can hospitals and other critical services operate without normal deliveries of oxygen, fuel, water, medicines and consumables?
- Which private organizations are essential to the response, and when did they last exercise with government?
- How will warnings reach people who do not speak Arabic or English, have limited digital access or require accessible formats?
- When did the executive team last make real-time decisions in an exercise with incomplete and conflicting information?
- How many corrective actions from the last exercise or emergency remain open, and who is accountable for closing them?

The Middle East can set a global benchmark for resilience

The Middle East has a compelling platform for global leadership in preparedness: strong national ambitions, major infrastructure investment, sophisticated aviation and logistics systems, expanding digital capability, extensive mass-gathering experience and the ability in many settings to mobilize resources quickly. Saudi Arabia and the UAE are especially well positioned to help shape this standard through their transformation agendas, advanced infrastructure, global connectivity and capacity to convene government, healthcare and industry. The opportunity now is to connect these strengths into an integrated readiness system that can be demonstrated, measured and continuously improved.

The decisive step is to connect and compound what already exists. Public health intelligence must connect to emergency command. Health systems must connect to utilities and logistics. Cyber teams must connect to continuity and patient safety. Climate alerts must connect to employers, hospitals and public warning. Private providers must connect to national coordination. Exercises must connect to funded corrective action. Recovery must connect to long-term health-system strengthening.

Preparedness is strategic infrastructure. It protects lives, preserves confidence, limits economic loss, supports national security and allows societies to continue functioning under pressure. The organizations that perform best in a crisis are rarely those with the longest plans. They are those that have made authority clear, built trusted relationships, invested in practical capabilities and rehearsed difficult decisions before the emergency.

The standard can therefore be simple and demanding: not whether a plan exists, but whether the system can demonstrate performance. Can it detect? Can it decide? Can it coordinate? Can it communicate? Can it surge? Can it sustain? Can it recover?

The Middle East has the ambition, capability and momentum to move from strong plans to demonstrated performance - and from episodic response to enduring resilience.

Contact Us

Al-Ghaf Dynamics

One Business Centre
38th Floor, Media One Tower, Dubai Media City
Dubai, UAE

+971 04 439 6347

main@ghafdynamics.com

www.ghafdynamics.com