KPMG

KPMG 4Dinsights Immersive

Scenario exercising and learning platform

A KPMG Product for G-Cloud 15

KPMG – About us

Our UK Cyber team

We've worked with countless organisations across multiple sectors, including financial services, life sciences, healthcare, government, telecommunications, energy and natural resources, and legal services. Our clients range in sizes, span across geographies and industries and are subjects to various regulatory requirements and obligations.

330+ professionals

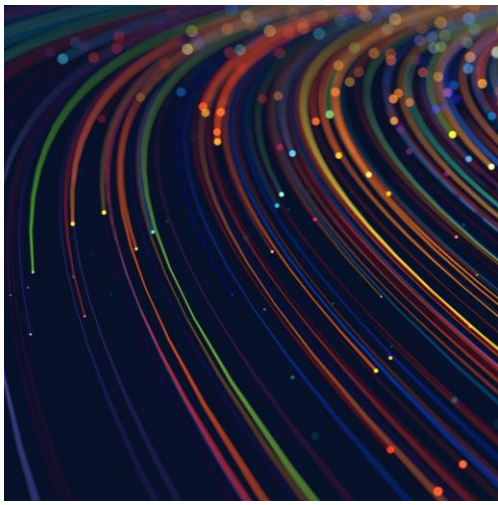
15 office locations

Part of a global team of 6200+ individuals

Our services

UK Cyber operates across 8 different service lines, catering to a wide range of governance and technical needs.

Cyber strategy	Cyber and enterprise resilience
Cyber tech transformation	Cyber defence services
Cyber risk	Privacy compliance
Identity and access management	Cyber incident response



Assured Service Provider

in association with National Cyber Security Centre

Cyber Incident Exercising

We are proud to be one of thee firms that has been granted the prestigious **NCSC Cyber Incident Exercise (CIE) Assured Provider status.**

"As a delivery partner for the NCSC CIE scheme, CREST is thrilled to congratulate KPMG on achieving Assured Provider status."

President of CREST.

Our Cyber team is complemented by our Connected Technology team.

We have access to a 2000-strong team of client-facing technologists combined with alliance partners, with a diverse range of skills and experience. This enables us to bring to our clients the most suitable resources, expertise and insights when needed.

We apply a data and technology driven approach to drive change through our digital transformation services.

KPMG Immersive scenario exercising and learning platform (4Di SaaS)

Service Description:

4Di is a scenario-based digital simulation and tabletop exercising platform that strengthens the resilience of government bodies, public sector organisations and multi-agency environments. It provides an immersive environment that supports structured learning, informed decision making and improved preparedness at all levels.

As the platform continues to evolve, 4Di is preparing to introduce advanced AI capabilities to support scenario creation, inject development and structured content generation, enabling faster production of high-quality scenarios and more consistent, scalable exercising programmes

What are the benefits of KPMG Immersive scenario exercising and learning platform (4Di SaaS)?

- Reduces time and resources needed to design and scale training and exercises.
- Delivers consistent, realistic scenarios for high-risk incident preparedness.
- Strengthens readiness through improved collaboration, decision making, and learning.
- Achieves cost efficiencies through automation, remote delivery, and repeatable exercises.
- Supports all seniority levels for organisation-wide and system-wide resilience.
- Scales across departments and regions to meet wider preparedness needs.
- Provides audit trails and metrics to support compliance and governance.
- Ensures secure handling of all training data and sensitive information

Our service features

- AI enables rapid creation of high-quality, customisable training scenarios.
- Realistic, time-pressured simulations improve operational decision making.
- Fully customisable scenarios, including injects, questions, and scenario flow, with support for up to 39 inject types.
- Supports a wide range of inject types and integrates with Google services and Slido.
- Enables remote and multi-agency sessions across locations.
- Automatically captures and securely stores participant inputs for audit and review.
- Browser-based access on any device across regions and languages.
- Provides a safe training environment with quick export to MELs and facilitator guides

More information can be found here https://kpmg.com/uk/en/home/services/products/4di.html

What 4Dinsight Delivers Out of the Box

Below is a snapshot of the available features, which can be fully customised to meet your specific requirements and branded in your own livery to deliver a tailored solution:

Scalable SaaS platform supports 1–500 participants per exercise with mobile and desktop access, enabling in-room, remote, or hybrid delivery.

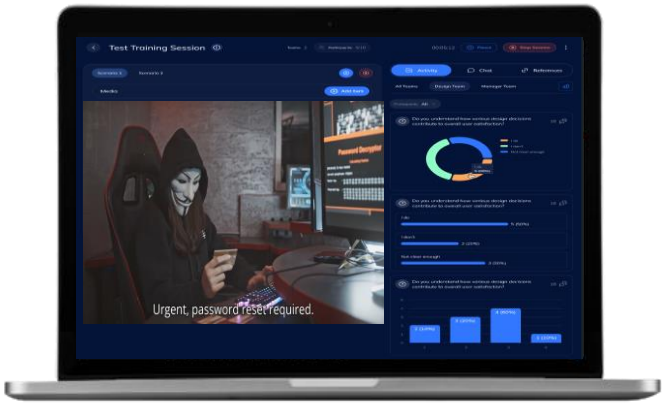
Realistic, pressurised crisis response through immersive learning. A scenario-based, threat-led approach builds and tests resilience in a safe environment.

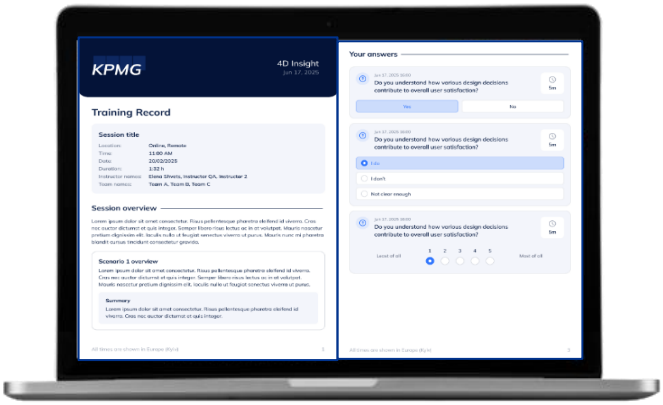
Supports continuous development & learning. Detailed reports provide insights into response effectiveness over time at individual and organisational levels.

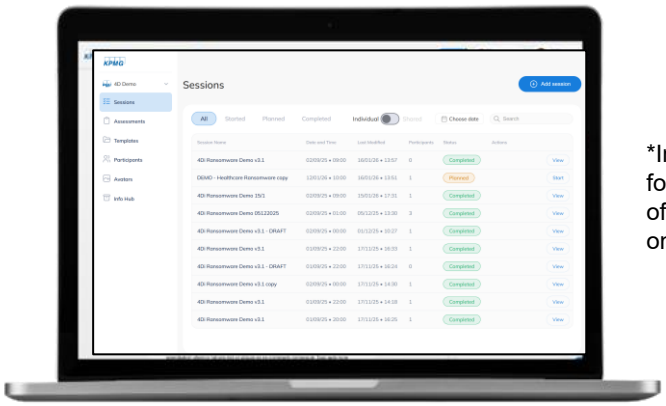
Platform-captured data and targeted questions, polls, and multiple-choice enable evidence-based findings and in-depth analysis of organisational response.

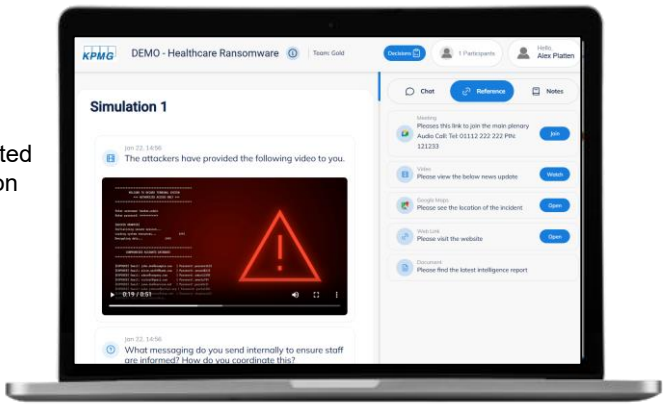
Smart inject formats, including audio calls, social media, emails, images and video create dynamic engagement to drive focused decision-making.

AI-driven scenario generation, taking the latest information on best practice and real-world context to enhance the experience and results.



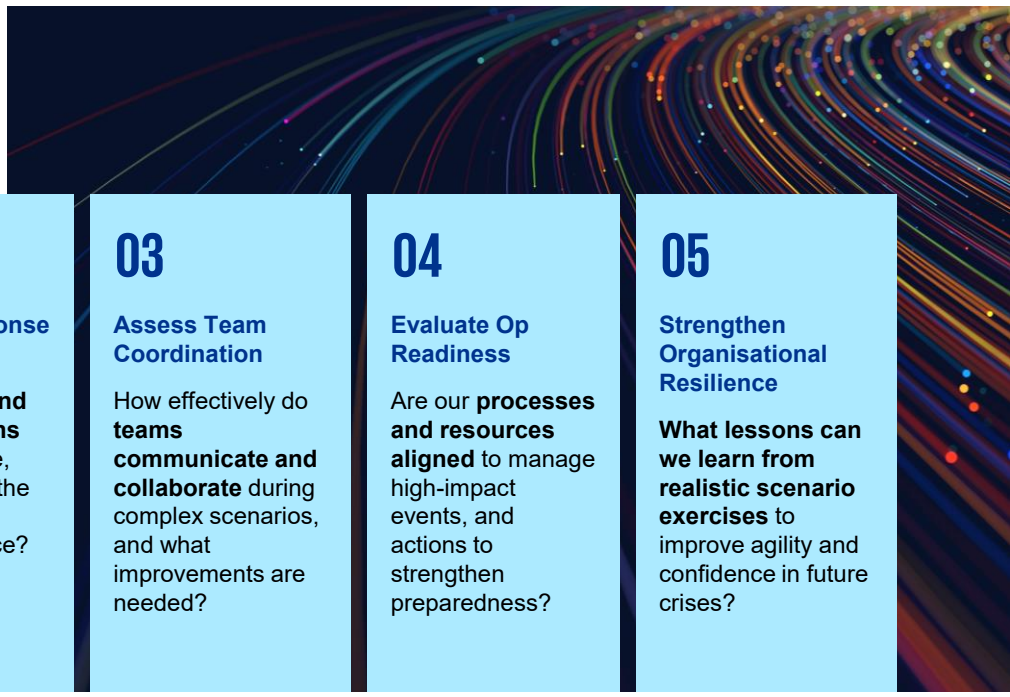






*Images generated for representation of the features only.

Use cases and Illustrative Scenarios



01

Test Strategic Decision-Making

How will **leadership respond under pressure** during a major disruption, and what decisions will shape recovery?

02

Validate Response Plans

Do our **crisis and continuity plans** work in practice, and where are the gaps that could impact resilience?

03

Assess Team Coordination

How effectively do **teams communicate and collaborate** during complex scenarios, and what improvements are needed?

04

Evaluate Op Readiness

Are our **processes and resources aligned** to manage high-impact events, and actions to strengthen preparedness?

05

Strengthen Organisational Resilience

What lessons can we learn from realistic scenario exercises to improve agility and confidence in future crises?

While below scenarios represent common threats faced by most organisations, not all may be equally relevant to your specific context or business unit. You do not need to select all scenarios during the assessment scoping process; when develop a scenario tailored specifically to your organisation needs

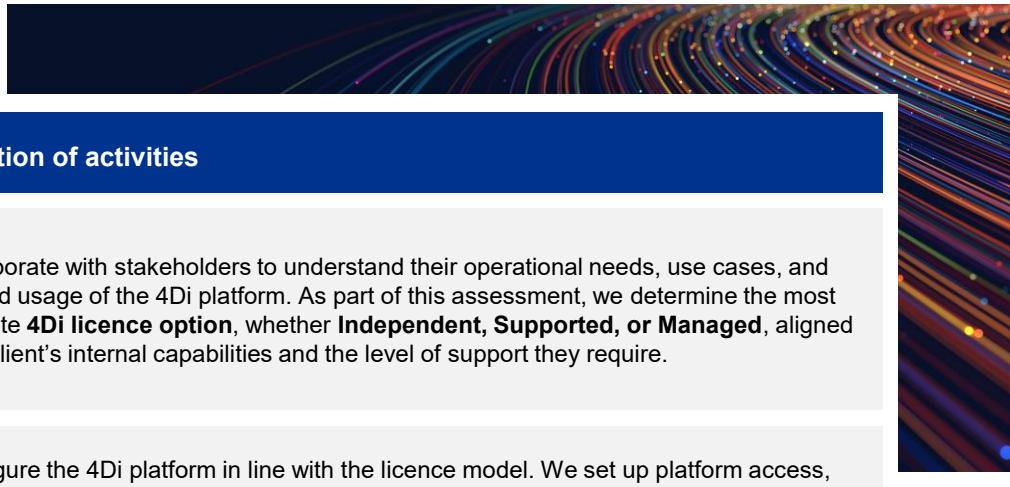
- Regional Power Failure and Infrastructure Loss
- Critical Supply Chain Disruption
- Coordinated Physical Attack or Geopolitical Incident
- Major Cyber Attack and Data Breach

Technology

- Accidental data disclosure
- Accidental digital services compromise
- Business email compromise
- Cloud environment outage/compromise
- Distributed Denial of service
- External major data breach
- Insider data breach
- Insider major data breach
- Insider software compromise
- Third party compromise
- Web framework compromise
- Widespread ransomware

Our Approach

Our approach enables rapid deployment of the 4Di platform, with many clients going live only days after contract signature. Because each organisation has different needs and levels of internal capability, we begin with a focused scoping exercise to understand how the platform will be used and to agree the most suitable **4Di licence option**, whether **Independent, Supported or Managed**, ensuring the deployment approach fits the level of support required.



Phase	Description of activities
1. Scoping	We collaborate with stakeholders to understand their operational needs, use cases, and forecasted usage of the 4Di platform. As part of this assessment, we determine the most appropriate **4Di licence option**, whether **Independent, Supported, or Managed**, aligned with the client's internal capabilities and the level of support they require. .
2. Deploy	We configure the 4Di platform in line with the licence model. We set up platform access, complete the initial configuration, and work with the client to identify the administrators who will manage the system. These administrators receive focused training to ensure they can access the platform and run exercises confidently. Once training is complete, we issue login credentials and confirm the client is ready to begin using the platform.
3. Support	Clients will be provided with a point of contact from KPMG who will be able to discuss use cases and any new development features of the platform. In the unlikely event of technical issues, a helpdesk will be available to provide clients with real time support.
4. Close	As the end of the contracted period approaches, we will agree with clients how we will mange the transfer of their data in line with contracted commitments.

Why KPMG

Case study 1 – Government Department

Client challenge

The client needed two immersive exercises to evaluate and strengthen their Silver (tactical) and Bronze (operational) response to a cyberattack, using a realistic scenario to test coordination and validate their new Business Continuity Incident Management Framework.

KPMG's response

- Worked with the client's business continuity and technology teams to create a cyber scenario tailored to their systems and risk profile.
- Delivered two hybrid exercises using the KPMG 4Di platform to drive real-time interaction, decision-making, and structured observation capture.
- Simulated a critical system outage to test tactical and operational response, escalation, communications, and governance.
- Guided participants through key decisions and discussions to surface interdependencies, strengths, and gaps.
- Summarised insights into clear, actionable recommendations to enhance incident response and business continuity maturity.

Value Delivered

- Improved understanding of tactical and operational response to ransomware.
- Clear visibility of gaps across governance, decision-making, and incident processes.
- Stronger learning through structured feedback and cross-team discussion.
- Increased awareness of Business Continuity documentation and future improvement needs.

Case study 2 – Training for police forces

Client challenge

A UK based police service needed to modernise its detective training, which relied on didactic teaching and a three-day paper-based scenario. The format lacked interactivity, made it hard for delegates to track individual decisions, and offered no personal performance records. The lengthy scenario also caused frustration and reduced engagement, highlighting the need for a more dynamic, realistic, and feedback-driven training approach

KPMG's response

- Introduced the 4Di web-based simulation platform to replace the traditional paper-based, didactic training approach.
- Implemented an individual incident log to help detectives record their hypotheses, decisions, and rationales throughout scenarios.
- Encouraged critical thinking and reflection by requiring each participant to document their decision-making process.
- Used the incident logs for assessment and structured feedback, enabling continuous learning and measurable individual progress.

Value Delivered

- Increased engagement and motivation through more realistic, streamlined scenarios.
- Strengthened critical thinking and decision-making skills via individual logging and reflection.
- Enabled clear, data-driven performance insights to support personalised development.
- Delivered a more interactive and impactful learning experience that accelerates professional growth.

Case study 3 – Government department

Client challenge

A UK government department asked KPMG to deliver a major cyber incident exercise for its Executive Committee. As leaders responsible for national security, law enforcement, and immigration, the ExCo needed an immersive understanding of how a serious cyberattack could impact the organisation targeting sensitive data, critical infrastructure, and national-level decision-making

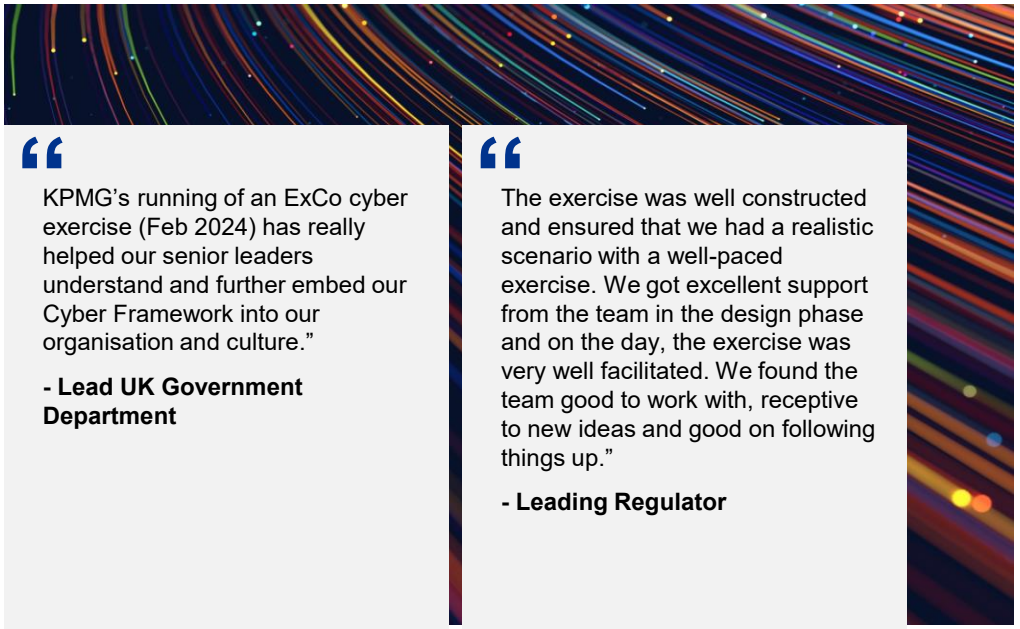
KPMG's response

- Designed and delivered a tailored senior-leadership cyber incident scenario using the 4Di platform.
- Worked with NCSC and Cabinet Office representatives to assess risk-based decision-making, options analysis, and prioritisation of critical activities across ExCo, departmental portfolios, and wider HMG.
- Tested communication flows and strategic messaging between ExCo and key internal and external stakeholders, including suppliers, law enforcement, regulators, and third-party partners.
- Provided structured insights and recommendations to strengthen governance, coordination, and executive-level cyber incident readiness.

Value Delivered

- Strengthened ExCo's understanding of major cyber risks and their potential organisational impact.
- Improved executive decision-making by allowing leaders to experience consequences in a safe, realistic simulation.
- Increased confidence in roles, responsibilities, and escalation during high-pressure incidents.
- Highlighted priority improvement areas, enabling a more proactive and resilient approach to cyber risk.

Why Clients Trust 4Di — In Their Own Words



Participants praised the simulation as innovative, immersive, and practical, with real-time injects and dynamic scenarios that created realistic decision-making challenges, strengthened collaboration between technical (bronze) and strategic (gold) teams.

The platform was described as 'excellent,' 'interactive,' and 'educational'. "

- A National Agency

KPMG's running of an ExCo cyber exercise (Feb 2024) has really helped our senior leaders understand and further embed our Cyber Framework into our organisation and culture."

- Lead UK Government Department

The exercise was well constructed and ensured that we had a realistic scenario with a well-paced exercise. We got excellent support from the team in the design phase and on the day, the exercise was very well facilitated. We found the team good to work with, receptive to new ideas and good on following things up."

- Leading Regulator

It was innovative and efficient. Very relevant."

"Provided real life incident response way through bronze and gold decision making level and also methodology way of handling a cyber crisis."

"It's very easy to use and makes you understand the concepts better."

"Practical, simulated the cyber crisis seamlessly and can be used by all level of cyber crisis management teams."

"The scenario was like real time based. It is a great platform for training more simulations."

"4Di tool really outlines the simulation thoroughly and effectively and helped in easy breakdown of the incident."

"4Di was realistic and team-focused. Its helps in decision-making, crisis response, and cyber readiness through hands-on simulation."

"The 4Di tool made the whole training engaging as it provided a clear understanding of crisis communication between strategic level decision."

- Government of Kenya/FCDO:

Infinitely better than a paper feed and the video clips, maps, etc make it a more immersive experience."

- Senior Police Commander

Great system for capturing input and serving injects; the IT worked brilliantly and I would definitely recommend using this approach for future exercises."

- CISO, Government Department

Engaging modern approach and accessible to all users with relative ease."

- C Level Health Executive

The best-structured exercise I've attended."

- UK Healthcare

kpmg.com/uk

Document Classification: KPMG Confidential

CREATE. | CRT164925A January 2026