Deloitte.

Together makes progress

When AI stops:

Operational resilience in an AI world

August 2026

Introduction

Deloitte's 2026 State of AI in the Enterprise report found that 64% of companies are starting to use AI to *deeply transform their business,* or *redesign key processes around AI*.[1]

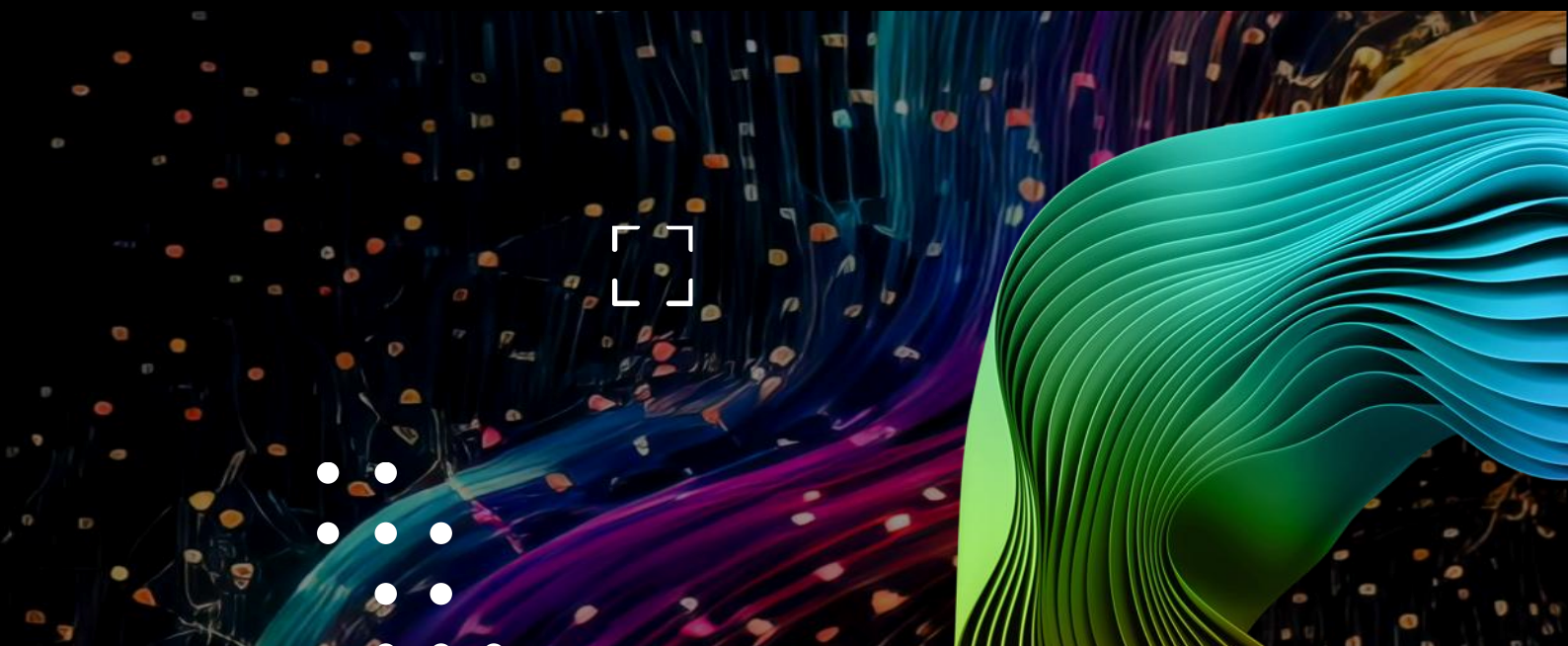
At the same time, technology-related disruption is increasing. Recent estimates put the annual cost of technology downtime for Global 2000 organisations at nearly $600 billion[2].

The need for effective AI governance and responsive capabilities has never been greater.

As artificial intelligence (AI) becomes embedded within critical business services, organizations must **adapt their approach to operational resilience**, recognising the **unique risks, behaviours**, **dependencies**, and **failure modes** associated with AI, and criticality of successful rollouts.

> *"Effectiveness, trust and stakeholder support for initiatives are critical to the success of AI transformation. For highly visible technologies, a relatively small amount of downtime can result in large financial, operational, legal and reputational impacts, disproportionately amplified by misinformation."*

Author's note: This article uses an all-encompassing term for AI. However, the risks, resilience challenges, and response options will vary depending on the form of AI which is being implemented (e.g. Agentic AI, Physical AI, or Generative AI).



What leaders need to know

At its most basic level, AI is no different to many other technologies. It depends on hardware, software, infrastructure, data and third parties to function, and shares many of the same vulnerabilities to disruptive risks (*see Diagram 1*). Many of the foundational concepts of operational resilience apply directly to AI-enabled services. The core principles: building capabilities to **anticipate disruption**, **absorb shock**, and **adapt** to mitigate impacts remain relevant.

But there are significant differences from traditional technology. AI capabilities are more exposed to rapidly changing risks, including sovereignty, regulation and capacity of infrastructure.

Within organisations, AI presents unique failure modes such as model drift and hallucinations, which can silently degrade the service without visible disruption.

Governance is not keeping up with the pace of change in AI. Many organisations lack the human and technical infrastructure to give visibility of all AI use cases and their associated risks. Without this, single-points-of-failures may not become visible until disruption occurs.

For high-profile use cases, the cost of AI-related disruption may extend beyond financial impacts. Public sentiment is still evolving, and a small amount of disruption has the potential to impact trust and adoption.

Leaders must recognise that disruption is going to occur, and plan accordingly.

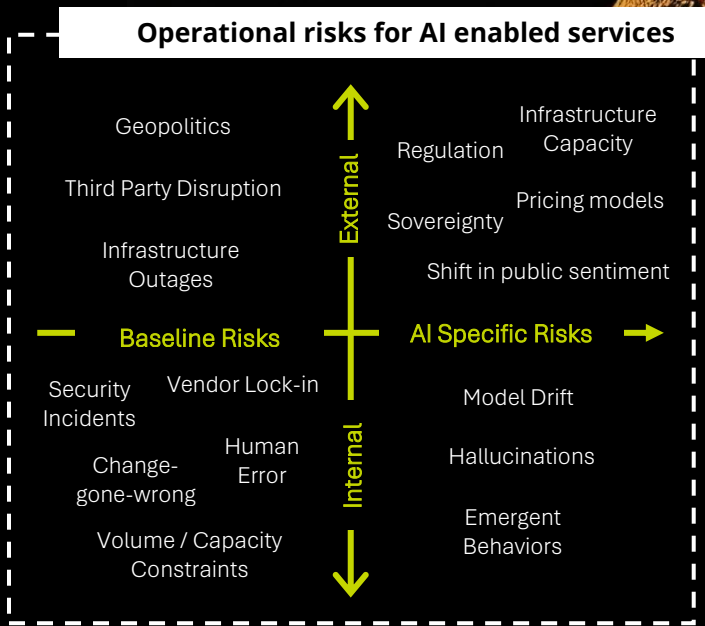


Diagram 1

Resilience challenges

This article groups AI resilience challenges into three key themes.

1. ***Trust is critical and fragile***
   For emerging technologies, loss of confidence can result in disproportionate impacts.

   Traditional technology failures are often visible and binary. A server is available or unavailable. A database is functioning or not functioning. Resilience planning often focuses on availability: the need for systems to be accessible and available.

   In contrast, AI systems may remain *technically operational* while producing increasingly *poor outcomes*. The system may remain available, but confidence in its abilities declines.

   For example, model drift impacting efficacy, reduced prediction accuracy, or emerging bias in decision-making could all impact the outcomes delivered by AI. A model can fail operationally because the underlying data has changed, become corrupted, or ceased to reflect real-world conditions.

   If not adequately monitored and detected, this has the potential to result in:
   - Incorrect automated decisions
   - Harm to stakeholders (e.g. customers or the wider public)
   - Regulatory, legal and contractual breaches
   - Financial impacts: For organisations operating in the EU, failures to monitor AI use cases can already result in penalties of up to 7% of global turnover (under the EU Artificial Intelligence Act)
   - Communication challenges, with the potential for issues to be distorted or amplified by misinformation
   - Reputational harm for the wider organisation
   - Downtime or disruption of service, if emergency interventions are required.

   Critically, any perceived loss of accuracy or reliability can significantly impact stakeholder trust in the use of AI.

What does this mean in the real world?

Illustrative scenario: Model drift

Scenario

- *A study used a machine learning model to predict whether patients arriving at the emergency department would need hospital admission. When COVID-19 began, patient characteristics and reasons for attending the emergency department changed dramatically, creating both **data drift** and **concept drift**.*

Impacts

- *Prediction accuracy declined, and the model became less reliable at identifying patients who needed to be admitted.*[3]

2. ***Rapidly evolving risks***
Hardware, software and infrastructure can fail. Energy, sovereignty and regulation present unique, disruptive challenges.

No technology is immune to failure. AI shares the same dependencies on hardware, software, infrastructure, data and third parties to function. Disruption to any direct (or indirect) assets in its supply-chain could result in a loss of service.

However, as a powerful and rapidly developing technology, AI is exposed to significantly more volatile risks. Each of these could result in a scenario where embedded AI is temporarily, or permanently, unavailable.

Loss of service may come as a result of constraints outside the organisation. For example:

- **Unavailability of critical dependencies** (hardware, software, infrastructure, data, third parties).
- **Geopolitics**: Trade disputes, conflicts, or sanctions all have the potential to delay or reduce the availability of critical hardware or materials.
- **Sovereignty**: Export controls or sanctions may restrict access to hardware, models, software, limiting the ability to develop or deploy AI systems.
- **Regulation:** Regulators, including the FCA, are actively reviewing risks presented by the use of AI, and there is growing recognition that regulation will need to adapt to the challenges. New laws may restrict where AI can be deployed, how data is processed, or which providers can be used.
- **Security threats/ vulnerabilities:** Triggering proactive measures to isolate impacts.
- **Lack of infrastructure capacity:** Restrictions on usage triggered by lack of energy, computing power, or grid capacity.

What does this mean in the real world?

Illustrative scenario: Energy infrastructure

Scenario

- *In 2025, the CEO of a multi-national technology company stated that its ability to expand AI services was constrained by lack of connected, powered datacentre capacity. "It's not a supply issue of chips, it's the fact that I don't have warm shells to plug into".* [4]
- *Multiple countries have introduced restrictions or conditions on new data centre connections. In 2021, Ireland introduced a moratorium on new data centres after warnings around grid capacity. Electricity demand for data centres grew from 5% of Ireland's electricity usage in 2015 to 22% in 2024. This was lifted in 2025, replaced with strict controls and restrictions on new data centres.*[5] *Similarly, Amsterdam and Singapore have introduced restrictions on the development of new data centres, with active debate in other countries.*

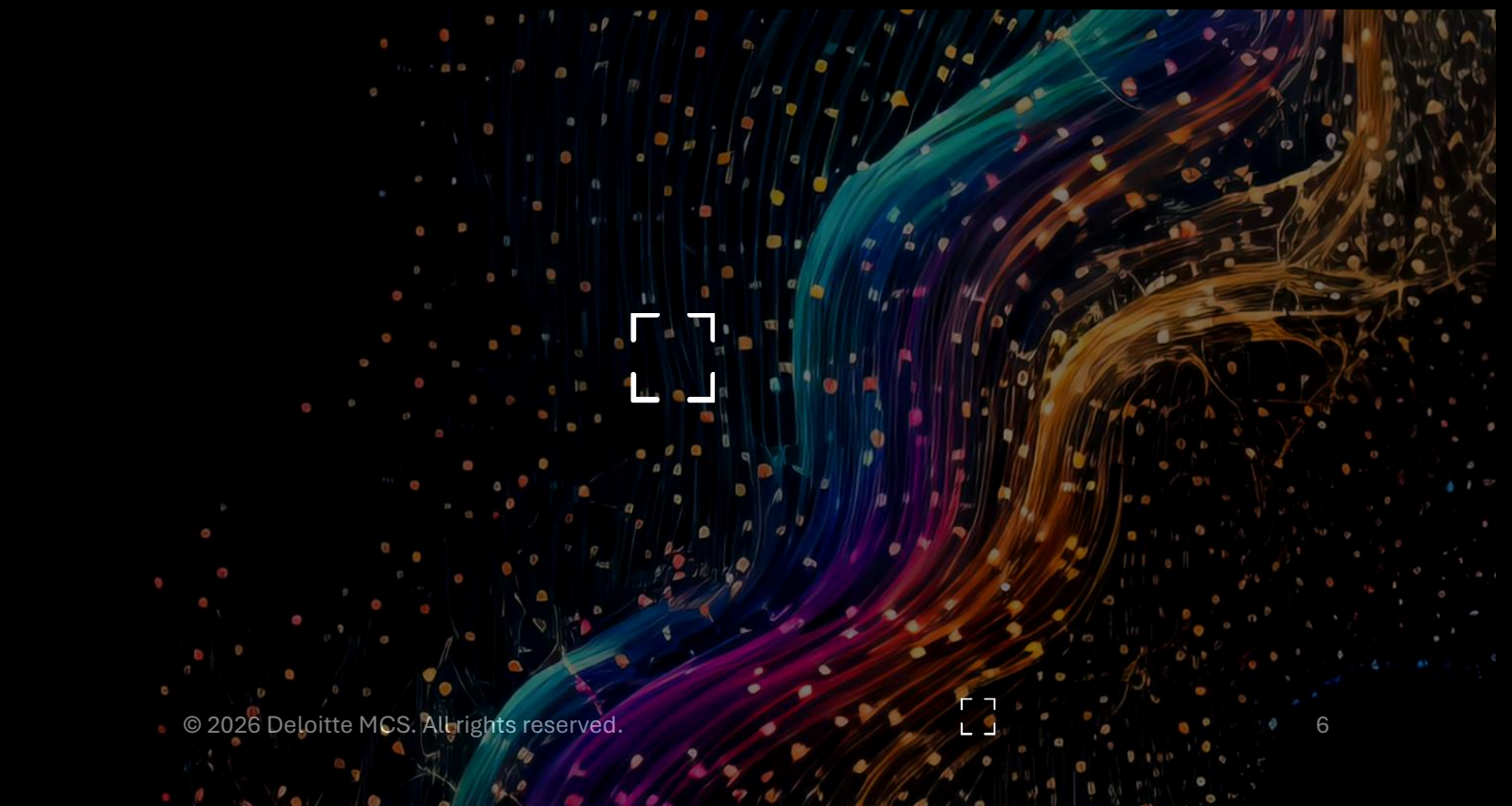
Impacts

- *Restrictions on grid connections and energy usage restricts the ability of AI providers to open or expand data centres. Whilst not yet evidenced, as adoption increases this may result in capacity constraints- e.g. providers are unable to meet demand in peak periods.*

Or, organisations may be presented with issues which force them to rapidly decouple from an embedded provider or technology. For example:

- **Shifts in pricing model:** Third-party providers may shift pricing models, leading to a scenario where the value gained from AI no longer exceeds the cost to the organisation. Pricing models may adapt to reduce consumption, manage demand or fund additional infrastructure required to meet needs.
- **Public sentiment:** Opinion on AI is still forming, and activist groups may influence views on individual providers or the technology as a whole. Many organisations are not equipped to communicate in response to these issues, with little or no visibility of their use cases, benefits and controls across the enterprise. In extreme cases, organisations may face intense pressure to remove a third-party provider of AI, or reduce exposure to AI in its entirety.
- **Vendor incompatibility**: Organisations may need to decouple from a provider or AI technology as a whole. This could be as a result of the previously listed risks, or for example; where a third-party provider no longer aligns with the organisation's values, where mergers or acquisitions change the sovereignty of a provider, or the security posture changes. If not prepared for in advance, this presents a significant engineering effort.

As organisations move from simple use cases to deeply embedded AI transformation, disruption to AI assets have the potential to create major impacts.



3. ***The recovery challenge***

AI services depend on complex models to process data, develop and produce an output. Organisations may procure external models, develop their own in-house, or purchase Software-as-a-Service platforms which meet their requirements.

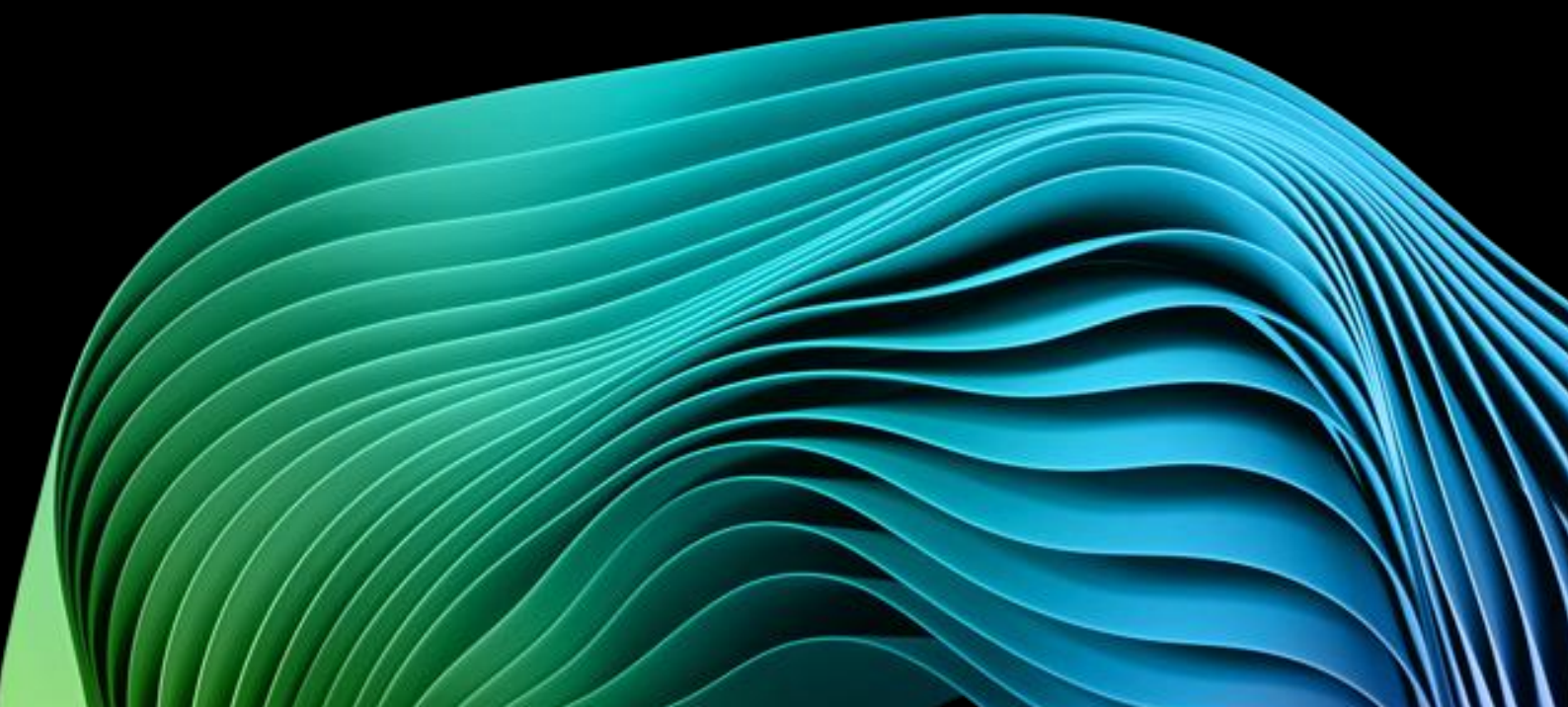
As elsewhere, resilience can be built by introducing redundancy (running two assets in parallel, e.g. third-party providers, machine learning models or data centres) or modularity (e.g. building additional capacity so components are able to take on extra load in the event of failure).

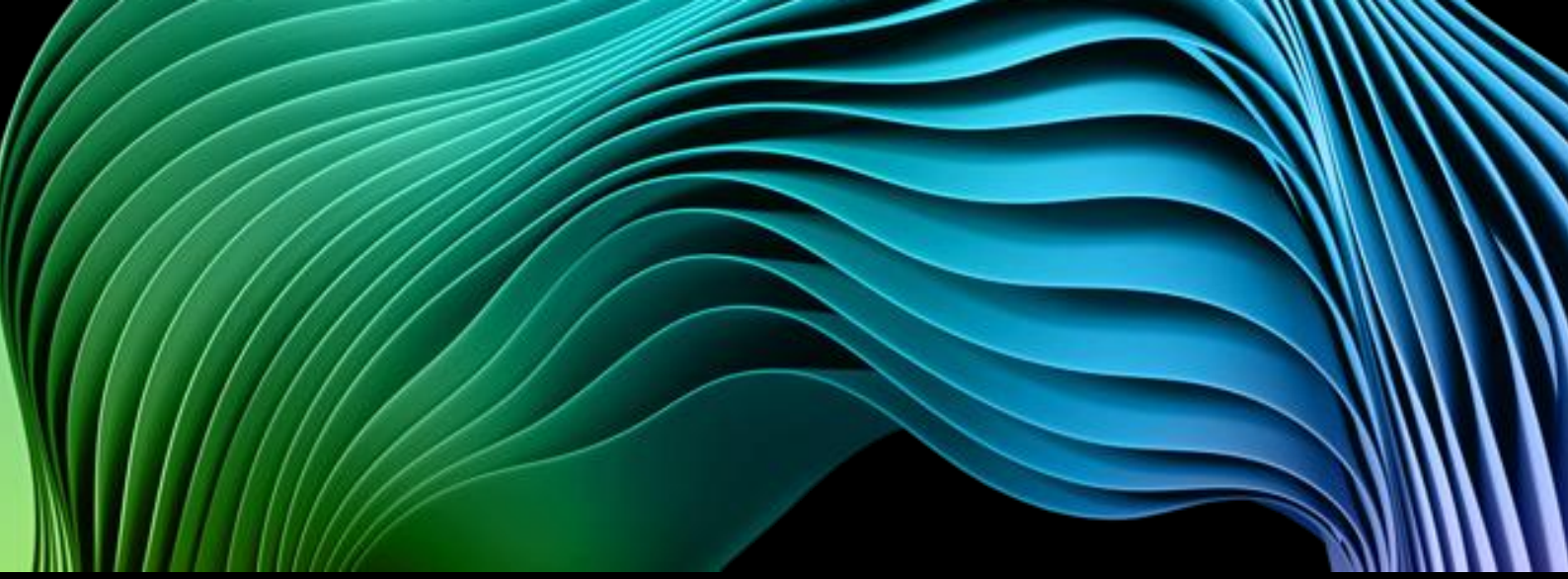
However, cost constraints often prevent organisations from running dual systems in parallel. This leaves a gap usually filled by contingency plans, which define alternative (often offline) routes to deliver services, and set out the limitations and risks associated with each response. For example, a bank may divert customers into branches in the event of a major IT system outage but be unable to deliver full capacity. They may choose to maintain branches or staff to retain this failsafe, assuring delivery of regulatory obligations.

This is where AI presents a dichotomy. As with other major technological advances, over time AI will replace or displace skills in the organisation.

As skilled professionals are replaced by technology, the failsafe of manual workarounds becomes less robust. As use of AI increases over time, the skills gap is likely to further build. Skills cannot be rapidly created in a major incident; they must be maintained over time.

In addition, the business processes used to train the AI will no longer exist. In a worst-case scenario, organisations may lack the data essential to rebuild their AI systems.





What actions should organisations take

To address these risks, organisations must proactively build the capabilities to **anticipate**, **absorb** and **adapt** for AI disruption.

Leaders should adopt a strategic approach to AI resilience, with the objectives of:

- Protecting people,
- Ensuring legal, regulatory and contractual compliance,
- Safeguarding investment,
- Minimising downtime,
- Mitigating the impacts of disruption, and
- Preserving stakeholder trust in new capabilities.

Any strategy for AI operational resilience must include:

1. *Trust as a measure of performance*
   Trust in AI-enabled services will be maintained not just through availability, but also accuracy, efficacy, and the framework to *respond effectively* in the event of degradation or disruption of service. To do this, organisations must develop:
   - **Appropriate governance**, establishing controls around AI across the organisation.
   - **Metrics, reporting and management information** which go beyond availability to measure trust in key outcomes, considering accuracy, useability and stability.
   - **Runtime monitoring,** utilising secondary AI tools to report against metrics and identify deviation.
   - **Defined thresholds** for incidents, outlining tolerance for variance against performance indicators and clear parameters for activating contingencies.
   - **Continuity plans**, including manual interventions, break-glass procedures in the event of catastrophic loss, and impacts on service, stakeholders, finance, legal and regulatory obligations.
   - **Communication plans** which reflect the risks faced by AI-enabled services, address potential for misinformation, and support organisations to rebuild confidence following degradation or disruption.

All of these capabilities must be tested against severe but plausible scenarios, gradually building collective skills and knowledge across the organisation.

2. *A long-term view of risk*
   The organisations that successfully adapt their resilience strategies will be better positioned to capture the benefits of AI while maintaining reliability, accountability, and stakeholder trust in the long-term. Investment in AI must be protected with a long-term approach to resilience. To do this, organisations must:
   - **Identify longer-term risks** and consider these against the risk appetite of the organisation. External risks such as geopolitics, regulation, sovereignty and limitations on wider infrastructure capabilities must be considered in architectural design decisions, alongside vendor changes in pricing model or supplier insolvency. Risks should be actively discussed and overseen by leadership.
   - **Encourage an impact-focused assessment of risk.** The criticality of services must be considered when evaluating exposure to risk. In a rapidly changing and volatile risk landscape, impact provides a consistent assessment criterion.
   - **Adapt for heightened sensitivity.** Any new initiative faces a period of increased sensitivity. Risks which may be tolerated in established technology may be heightened in new programmes of AI deployment. Where successful adoption (and the AI investment) relies upon trust, resilience must be built through multiple measures (including architectural design decisions and proportionate command, control and communication structures).
   - **Establish horizon scanning and risk monitoring** to track risks and actively build contingencies as new scenarios emerge.

3. *Embedding Resilience by Design*
   A robust approach to resilience will assume that disruption *will* occur, and that it will not be possible to predict or prevent every scenario. Whilst AI presents multiple new 'triggers' for disruption, the outcome is the same as other technologies- a loss of critical infrastructure, potentially causing wide-ranging impacts. Leaders must embed resilience into the design and delivery of services:
   - **Align contingencies with criticality.** As organisations increasingly deploy AI in critical business services, operational resilience frameworks must reflect the criticality of outcomes AI is used to deliver. Assessments must evaluate the impacts of disruption, both internal and external, in worst-case scenarios. Identifying and prioritising critical outcomes, understanding dependencies, identifying risks, building contingencies and conducting scenario testing continue to provide a strong foundation.
   - **Implement Resilience by Design** principles into the architecture of systems: seeking to reduce the impacts of disruption by actively building modularity, diversity, redundancy and adaptability. Design discussions should include ways to reduce or mitigate single-points-of-failure (e.g. by running two parallel systems), and actively consider future requirements (e.g. flexibility to avoid vendor lock-in). By actively building resilience from the outset, organisations can consider the 'what if' scenarios, and establish architectural standards which build flexibility, redundancy and modularity.
   - **Embed resilience at all levels of the organisation**, from technology architecture to procurement and commercial functions, ensuring decisions with long-term implications align with the organisation's overarching risk tolerance.

How can we help

Deloitte's Reputation, Crisis and Resilience team are recognised leaders in resilience. We have deep expertise in operational resilience, business continuity, risk, incident and crisis management, with applied experience designing and implementing operational resilience capabilities in live service environments.

We frequently work with C-Suite and Boards to identify operational risks, develop resilience and respond during major incidents. Our approach to AI resilience brings together experts in AI, Governance, Engineering, Resilience, Communications, Risk and Crisis/ Incident Management to provide deep analysis and broad perspectives.

Our Trustworthy AI governance services give our clients the confidence their AI is safe, robust, responsible and compliant. Our expertise covers validation, standards, regulation and compliance, ethics, risks and controls, strategy, implementation and operation. We help organisations identify risks, develop or scale their governance, and help align them with standards such as ISO42001.

Contacts

Sarah Black
Partner | Reputation, Crisis & Resilience
sarahblack@deloitte.co.uk

Kat Bitterli
Associate Director | Reputation, Crisis and Resilience
kbitterli@deloitte.co.uk

Kevin Macnish
Associate Director | Trustworthy AI
kmacnish@deloitte.co.uk

References

1. Deloitte, 'State of AI in the Enterprise', *Deloitte*, (2026), (Last Accessed 14/08/2026), Available at https://www.deloitte.com/uk/en/issues/generative-ai/state-of-ai-in-enterprise.html .
2. Splunk, 'The Hidden Cost of Downtime 2026: A $600 Billion Wake-up Call', *Oxford Economics*, (2026), (Last Accessed 10/08/2026), Available at https://www.splunk.com/en_us/form/the-hidden-costs-of-downtime.html .
3. Duckworth, Christopher, Chmiel, Francis, Burns, Dan, Zlatev, Zlatko, White, Neil, Daniels, Thomas, Kiuber, Michael, and Boniface, Michael, 'Using explainable machine learning to characterise data drift and detect emergent health risks for emergency department admissions during COVID-19', *Scientific Reports,* 11(1), 23017 (2021), (Last Accessed 06/08/2026), Available at https://pmc.ncbi.nlm.nih.gov/articles/PMC8626460/?utm .
4. B2g Pod, 'All things AI w @altcap @sama & @satyanadella', *Youtube,* (2025, Oct 31) (Last Accessed 14/08/2026), Available at https://youtu.be/Gnl833wXRz0?si=wwMW-PadCKFxl-j6 .
5. Commission for Regulation of Utilities, 'The CRU Publishes its Decision on New Electricity Connection Policy for Data Centres', *CRU,* (2025), (Last Accessed 10/08/2026), Available at https://www.cru.ie/about-us/news/the-cru-publishes-its-decision-on-new-electricity-connection-policy-for-data-centres.