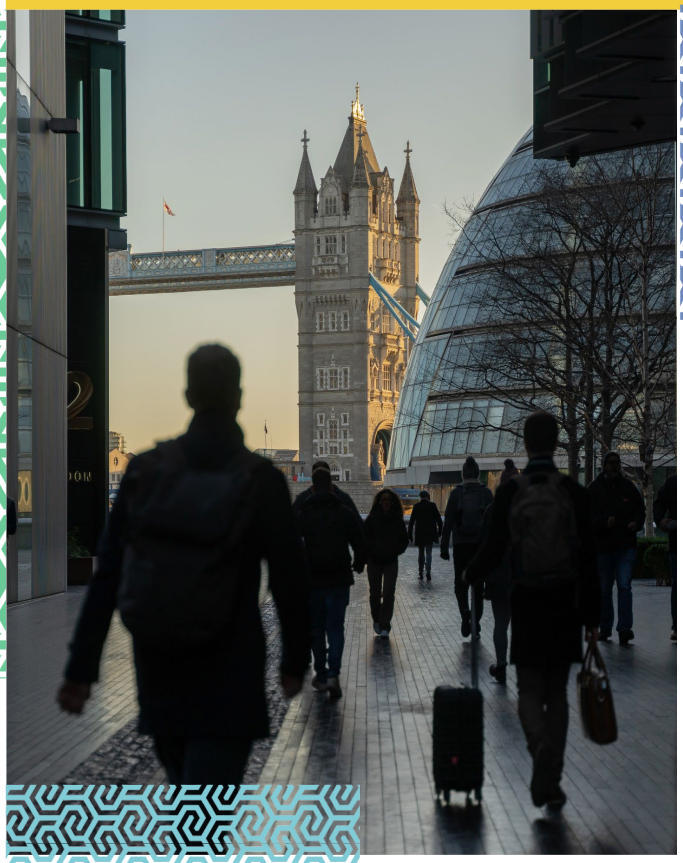
rmp education

# Risk Control

## Public Sector

State of the Nation Report 2024



In partnership with

GALLAGHER BASSETT
GUIDE. GUARD. GO BEYOND.

**Risk Management Partners**
rmpartners.co.uk

# Contents

# 1 The State of the Nation Report 2024

Welcome to the State of the Nation Report 2024 produced by RMP Risk Control for the Public Sector. This document represents the second iteration of the report. The report will be updated and republished on an annual basis.

The Global Risks Report 2024[1], which considers risks that maintain the potential to negatively impact a significant proportion of global GDP, population or natural resources, predicted 2024 would experience a continuation of rapid technological advancements and economic uncertainty. This would be compounded by two ongoing major crises associated with climate change and geo-political conflict. Tensions and active hostilities in various regions around the world would lead to increased insecurity. Simultaneously, nations would struggle with the effects of extreme weather, as efforts for climate-change adaptation fell short of addressing the scale of the problem. Cost-of-living pressures would persist due to high inflation and interest rates, causing further economic uncertainty. Negative headlines would continue to fuel growing societal frustrations and polarisation, compounded by risks, such as misinformation and disinformation.

The top five 'current risks' presented by the Global Risk Report 2024 were:

1. Extreme weather
2. AI-generated misinformation and disinformation
3. Societal and / or political polarisation
4. Cost-of-living crisis
5. Cyberattacks

As we know, the Public Sector do not operate within a vacuum and so would maintain significant exposure to these risks.

At an industry level, The Allianz Risk Barometer 2024[2] predicted a similar array of risk exposures from 2024. Risks such as digitalisation, climate change, and an unpredictable geopolitical landscape maintaining the potential to impact organisations. These risks would manifest through a continuation of extreme weather events, ransomware attacks, and regional conflicts, challenging the resilience of supply chains.

The top five risks at an industry level in 2024 were:

1. Cyber incidents (e.g., cyber-crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)
2. Business interruption (including supply chain disruption)
3. Natural catastrophes (e.g., storm, flood, earthquake, wildfire, extreme weather events)
4. Changes in legislation and regulation (e.g., tariffs, economic sanctions, protectionism, Euro-zone disintegration)
5. Macroeconomic developments (e.g., inflation, deflation, monetary policies, austerity programs)

Throughout 2024 the Public Sector faced several very familiar major challenges, including:

- **Budget constraints**: The Public Sector was once again operating under challenging financial pressures, constantly striving to balance limited resources with growing service demands. Since the Local Government Finance Act of 1988, fourteen councils have issued Section 114 Notices, with twelve of these occurrences happening since 2017
- **Increasing demand for services**: The Public Sector continued to experience heightened demand for services due to factors such as population growth, demographic shifts, including an ageing population, and evolving societal needs. Meeting these demands within the confines of limited budgets necessitated effective strategic planning and innovative solutions.

- **Political and policy changes**: The change in Central Government administration, such as the move from Conservative to Labour in 2024, will often maintain significant implications for the Public Sector, potentially affecting policies, priorities, and funding allocations. An example of this was provided in the form of the Labour Government's announcement of ambitious new plans for local government reorganisation, with the intention to streamline structures, improve efficiency, and alignment of local governance with devolved powers
- **Technological advancements**: The rapid pace of technological change continued to pose ongoing challenges in keeping up with digital transformation, cybersecurity, while ensuring public services are accessible and efficient. Cybersecurity remains a critical concern, as Public Sector organisations are frequent targets for criminal enterprises and individuals due to the sensitive data they possess, their relatively high profile, the critical infrastructure they manage, and the potential for operational disruption that can be caused
- **Workforce challenges**: The Public Sector continued to face persistent difficulties in attracting and retaining skilled workers, particularly in fields such as healthcare, education, and technology. Workforce shortages adversely affect service delivery and organisational effectiveness

This report will seek to explore a spectrum of risks, both old and new, that presented significant challenges to the Public Sector in 2024 or which the Public Sector are likely to face in 2025.

# 2 Devolution and Reorganisation

The English Devolution White Paper, released in December 2024, outlined the government's vision for streamlined local government structures. This approach aims to achieve better outcomes for residents, save significant public funds for reinvestment in public services, and enhance local accountability[3].

**Devolution**

With the ambition of ensuring that decisions are made closer to local people, local communities, and local businesses, devolution seeks to transfer powers and funding from national to local government.

By devolving powers and funding to the local level, ultimately creating greater freedoms, it is anticipated that the results will include the creation of more effective public services and greater potential for growth in local regions.

**Risks Presented by Devolution**

Local government devolution, while offering numerous benefits, also presents several risks that need to be carefully managed:

- **Inconsistent service delivery:** Devolution can lead to variations in service quality and availability across different regions, as local governments may have differing capacities and resources
- **Financial risks:** Local governments may face financial challenges if they lack the expertise or resources to manage devolved funds effectively. This could lead to budget shortfalls or inefficient use of resources
- **Capacity and expertise:** Not all local governments may have the necessary expertise or capacity to handle new responsibilities effectively, potentially leading to inefficiencies or service disruptions
- **Accountability and governance:** With increased powers, there is a risk of reduced accountability if local governance structures are not robust. Ensuring transparency and accountability in decision-making is crucial
- **Inequality between regions:** Devolution could exacerbate regional inequalities if wealthier areas are better able to capitalise on devolved powers, leaving less affluent regions behind
- **Political fragmentation:** Devolution may lead to political fragmentation, with local governments pursuing policies that conflict with national priorities, potentially leading to tensions and inefficiencies
- **Coordination challenges:** Effective coordination between different levels of government is essential. Devolution can complicate this coordination, leading to potential overlaps or gaps in service delivery
- **Public resistance:** Changes in governance structures may face resistance from the public or local officials who are accustomed to existing systems, potentially hindering the implementation of devolved powers
- **Implementation costs:** Transitioning to a devolved system can incur significant costs, including restructuring expenses and investments in capacity building, which may strain local budgets
- **Risk of failure:** In cases where local governments are unable to manage devolved responsibilities effectively, there is a risk of failure in delivering essential services, which could impact public trust and wellbeing

To mitigate these risks, it is essential for local government to receive adequate support, training, and resources, and for there to be clear frameworks for accountability and coordination with the national government.

**Reorganisation**

The principal objective of these plans is to facilitate a transitional programme of local government reorganisation, moving away from the two-tier system of local government that currently exists across many regions in England, so that all council services in an area are delivered by a singular unitary council.

It is proposed, with exceptions considered, that new unitary councils should ideally serve a population of 500,000+ people. This will allow the new unitary councils to improve capacity and efficiency in service delivery.

Pre-existing unitary councils may also face reorganisation based upon performance (failure), size or boundaries.

**Risks Presented by Reorganisation**

Past experiences suggest that local government reorganisation, while aimed at improving efficiency and service delivery, can create several risks that need to be carefully managed:

- **Disruption to services**: The transition process may temporarily disrupt the delivery of services as new structures are implemented and staff adjust to changes
- **Financial costs**: Reorganisation can incur significant upfront costs, including restructuring expenses, investments in new systems, and potential redundancy payments, which may strain local budgets
- **Loss of local identity**: Merging councils or altering boundaries may lead to a loss of local identity and community representation, potentially alienating residents who feel disconnected from larger administrative units.
- **Resistance to change**: Staff, elected officials, and residents may resist changes due to uncertainty or attachment to existing structures, potentially hindering the implementation process
- **Complexity in integration**: Integrating different systems, processes, and cultures from multiple councils can be complex and may lead to inefficiencies or conflicts if not managed effectively.
- **Accountability and governance challenges**: Larger unitary councils may face challenges in maintaining accountability and ensuring that local needs are adequately represented and addressed
- **Potential for inequality**: Reorganisation may lead to disparities in service provision if resources are not equitably distributed across newly formed councils
- **Impact on workforce**: Changes in organisational structure may lead to job losses or changes in roles, affecting staff morale and potentially leading to a loss of experienced personnel.
- **Legal and regulatory Issues**: Navigating legal and regulatory requirements during reorganisation can be complex and may pose challenges if not carefully managed.
- **Risk of failure**: If reorganisation is not well-planned and executed, there is a risk that the intended benefits, such as improved efficiency and service delivery, may not be realised.

To mitigate these risks, it is crucial for affected organisations to engage in thorough planning, stakeholder consultation, and communication throughout the reorganisation process. Additionally, providing support and training for staff, ensuring equitable resource distribution, and maintaining transparency and accountability can help address potential challenges.

# 3 Cyber Threat

Cyber threat remains an on-going concern on a global basis.

The cyber threat in the Public Sector is significant. Government agencies and Public Sector organisations are prime targets for cyber-criminals due to the sensitive information that is held and the potential disruption that can be caused.

Some key cyber threats in the Public Sector include:

- **Data breaches**: Public Sector organisations often hold vast amounts of personal and sensitive information, making them attractive targets for cybercriminals seeking to steal data for financial gain or identity theft. Data breaches can be very costly
- **Ransomware attacks**: These attacks involve encrypting an organisation's data and demanding a ransom for its release. Public Sector entities are particularly vulnerable due to the critical nature of their services and the potential impact of operational disruptions. Several Public Sector organisations have suffered high profile ransomware attacks
- **Phishing and social engineering**: Cybercriminals frequently use phishing emails and social engineering tactics to deceive employees into revealing login credentials or other sensitive information, which can lead to unauthorised access to systems
- **Denial-of-service attacks**: These attacks aim to disrupt services by overwhelming systems with traffic, potentially causing significant downtime and affecting the delivery of essential public services
- **Insider threats**: Employees or contractors with access to sensitive systems may intentionally or unintentionally compromise security, leading to data leaks or system vulnerabilities
- **Supply chain vulnerabilities**: Public Sector organisations often rely on third-party vendors for various services, and vulnerabilities in these supply chains can be exploited by cybercriminals to gain access to government systems
- **Legacy systems**: Many Public Sector entities operate using outdated technology, which may lack modern security features and be more susceptible to cyber-attacks
- **Critical infrastructure risks**: Public Sector organisations manage critical infrastructure, such as utilities and transportation systems, which are attractive targets for cyber-attacks that can cause widespread disruption
- **Lack of resources**: Budget constraints may limit the ability of Public Sector organisations to invest in robust cybersecurity measures, leaving them vulnerable to attacks.
- **Regulatory compliance**: Ensuring compliance with relevant regulations and standards can be challenging, especially as threats evolve and new requirements emerge

To address these threats, Public Sector organisations must prioritise cybersecurity by investing in modern technologies, conducting regular security assessments, training employees on best practices, and developing comprehensive incident response and business continuity plans. Collaboration with cybersecurity experts and other government entities can also enhance resilience against cyber threats.

The UK Government has implemented various cybersecurity initiatives, such as the creation of the National Cyber Security Centre (NCSC)[4] and the Cyber Essentials Certification Scheme[5] which is an industry-supported scheme to help organisations protect themselves against common online threats.

# 4 Misinformation and Disinformation

Misinformation and disinformation have been identified as a significant global risk by the World Economic Forum[6]. It can impact how people perceive reality and make decisions. In the first instance, we should consider the definitions which subtly differentiate the two concepts

— **Misinformation**

Misinformation is false or inaccurate information that is spread without malicious intent. It often results from misunderstandings, misinterpretations, or mistakes.

While not intended to deceive, misinformation can still lead to confusion, misinformed decisions, and the spread of incorrect beliefs. It can affect areas such as public health, safety, and policymaking.

Examples of misinformation may include sharing incorrect statistics, outdated information, or misunderstood news reports.

— **Disinformation**

Disinformation is deliberately false or misleading information spread with the intent to deceive or manipulate. It is often used strategically for political, financial, or ideological purposes.

Disinformation can undermine trust in institutions, polarise communities, and influence public opinion and behaviour. It can be used to sway elections, damage reputations, or incite social unrest.

Examples of disinformation may include fabricated news stories, doctored images or videos, or coordinated campaigns to spread false narratives.

**Effects on the Public Sector**

Misinformation and disinformation may pose significant risks to the Public Sector, affecting governance, public trust, and the effective delivery of services:

— **Erosion of public trust**: Persistent exposure to false information can undermine trust in public institutions and officials, making it challenging for governments to effectively communicate and implement policies

— **Policy and decision-making challenges**: Misinformation can lead to poorly informed policy decisions if public officials rely on inaccurate data or public sentiment shaped by false narratives

— **Public safety risks**: Inaccurate information, particularly related to health and safety, can lead to harmful behaviours. For example, misinformation about vaccines or emergency protocols can result in public health crises or ineffective responses to emergencies

— **Social unrest and polarisation**: Disinformation campaigns can exacerbate societal divisions and fuel social unrest by spreading false narratives that polarise communities and incite conflict

— **Resource misallocation**: Responding to misinformation and disinformation can divert valuable resources away from essential public services, as Public Sector organisations may need to invest in countermeasures and public education campaigns

— **Impact on elections and democratic processes**: Disinformation can influence electoral outcomes by spreading false information about candidates, voting processes, or election results, undermining the integrity of democratic processes

— **Operational disruptions**: False information can lead to confusion and operational disruptions within Public Sector organisations, affecting their ability to deliver services efficiently

— **Reputational damage**: Public Sector organisations may suffer reputational harm if they are perceived as sources or victims of misinformation, affecting their credibility and authority

To mitigate these risks, Public Sector organisations need to prioritise transparency, engage in proactive communication, and collaborate with media, technology platforms, and civil society to combat misinformation and disinformation. Investing in media literacy programs and developing robust fact-checking and verification processes are also essential strategies to address these challenges.

# 5 Extreme Weather

In 2024, Earth experienced its highest average surface temperature ever recorded, as determined by a NASA-led analysis. Global temperatures that year were 2.30 degrees Fahrenheit (1.28 degrees Celsius) above NASA's 20th-century baseline average from 1951 to 1980, surpassing the previous record set in 2023. This new milestone followed an extraordinary 15-month period, from June 2023 to August 2024, during which each month set a new temperature record[7].

It is believed that the warming trend observed in recent decades is primarily caused by the accumulation of heat-retaining greenhouse gases, such as carbon dioxide and methane.

**Extreme Weather Events**

In 2024, extreme weather events impacted populations worldwide. Although not every event can be directly linked to climate change, it is understood that a warming planet will lead to an increase in their frequency.

Some notable examples included[8 9]:

- **Flooding**

  As temperatures rise, the atmosphere can retain more moisture, leading to more intense rainstorms and an increased risk of flooding across the globe.

  Devastating floods were experienced in Afghanistan, Pakistan, Spain, Brazil, Hungary, and the United Arab Emirates.

- **Wildfires**

  Numerous regions experienced severe wildfires in 2024, with North and South America facing particularly devastating impacts. The intensity of these fires was exacerbated by a combination of drought conditions and extreme heat.

  Catastrophic wildfires were experienced in Chile, Canada, United States of America, Mexico, Croatia, Portugal, and the United Arab Emirates.

- **Earthquakes and Landslides**

  The movement of tectonic plates over long periods of time causes energy to be generated by friction. Once the build-up of energy reaches a tipping point, the energy is released in the form of an earthquake.

  Some notable earthquakes occurred in 2024 in Japan and Taiwan.

  Earthquakes can cause geological instability which increases the chances of devastating landslides.

  Deadly landslides occurred in India and Papua New Ginea

- **Tropical Cyclones, Typhoons, and Hurricanes**

  Tropical cyclones are powerful spinning storms. Depending on where in the world they form, they are described using different names. Tropical cyclones, typhoons, and hurricanes are essentially the same type of storm.

  In 2024, devastating tropical cyclones occurred in the Philippines, Vietnam, China, Thailand, United States of America, Mozambique, Malawi, India, Kenya and Tanzania.

Extreme weather events can have significant impacts on Public Sector organisations, affecting their operations, infrastructure, and service delivery. Here are some key effects:

**Effects on Public Sector Organisations**

- **Operational disruptions**: Extreme weather, such as heavy snowfall, flooding, or storms, can disrupt the daily operations of Public Sector organisations. This can lead to closures of offices, schools, and other public facilities, impacting service delivery to the public.
- **Infrastructure damage**: Public Sector infrastructure, including roads, bridges, and buildings, can suffer damage from extreme weather events. This can result in costly repairs and maintenance, as well as potential safety hazards for employees and the public.

- **Increased demand for services**: During extreme weather events, there is often an increased demand for emergency services, healthcare, and social services. Public Sector organisations must be prepared to respond to these heightened needs, which can strain resources and personnel.
- **Financial implications**: The costs associated with repairing damage, implementing emergency measures, and managing increased service demands can have significant financial implications for Public Sector organisations. Budget reallocations may be necessary to address these challenges.
- **Impact on employees**: Extreme weather can affect the safety and wellbeing of Public Sector employees. Organisations need to ensure that their staff are protected and supported during such events, which may include flexible working arrangements or additional resources.
- **Community impact**: Public Sector organisations play a crucial role in supporting communities during extreme weather events. They are often responsible for coordinating relief efforts, providing shelter, and ensuring that vulnerable populations receive necessary assistance.

  Public Sector organisations need to develop and implement effective risk management strategies to mitigate the impacts of extreme weather. This includes investing in resilient infrastructure, creating emergency response plans, and ensuring continuity of operations.

# 6 Business Interruption

As mentioned previously within this report, the Allianz Risk Barometer 2024[2] suggested that 'Business interruption' (including supply chain disruption) was one of most important corporate concerns for 2024, with only 'Cyber incidents' (e.g., cyber-crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties) ranked above it.

As nearly every organisation depends on supply chains for the provision of essential products and services, the risk of business interruption and supply chain disruption continues to be a primary concern.

Business interruption within the Public Sector can have significant consequences, affecting the delivery of essential services and the functioning of operations. Here are some key aspects to consider:

- **Service delivery impact**: Interruptions can lead to delays or halts in the provision of critical services such as healthcare, education, emergency response, and social services, impacting citizens who rely on these services
- **Operational challenges**: Disruptions can affect the day-to-day operations of Public Sector organisations, including administrative functions, communication systems, and resource management, potentially leading to inefficiencies and increased costs
- **Infrastructure vulnerabilities**: Public Sector infrastructure, such as transportation networks, IT systems, and public facilities, can be vulnerable to disruptions caused by natural disasters, cyberattacks, or other unforeseen events
- **Financial implications**: Business interruptions can result in financial strain due to the costs associated with recovery efforts, emergency measures, and potential loss of revenue or funding
- **Impact on employees**: Interruptions can affect Public Sector employees, leading to changes in work arrangements, increased workloads, or job uncertainty. Supporting staff during disruptions is essential for maintaining morale and productivity

To effectively manage the risk of business interruption, Public Sector organisations need to consider two essential elements:

- **Risk management and preparedness**: Effective risk management strategies are crucial for minimising the impact of business interruptions. This includes developing contingency plans, investing in resilient infrastructure, and ensuring continuity of operations
- **Community and stakeholder engagement**: Public Sector organisations must engage with communities and stakeholders to communicate effectively during interruptions, ensuring transparency and maintaining trust.

Overall, addressing business interruption risks within the UK public sector requires proactive planning, investment in resilience, and effective response strategies to ensure the continuity of essential services and operations.

**Business Continuity Management**

Business Continuity Management (BCM) is a comprehensive approach that organisations use to ensure the continued operation of critical business functions during and after a disruption. It involves planning and preparation to manage risks that could lead to business interruptions, ensuring that essential services and operations can continue with minimal impact. The key components of BCM include:

- **Risk assessment and analysis**: Identifying potential threats and vulnerabilities that could disrupt operations, such as natural disasters, cyberattacks, supply chain failures, or pandemics. This involves evaluating the likelihood and impact of these risks
- **Business Impact Analysis (BIA)**: Determining the effects of disruptions on business operations and identifying critical functions and processes that must be prioritised for recovery. This helps in understanding the potential consequences of interruptions

- **Strategy development**: Creating strategies to mitigate identified risks and ensure the continuity of critical operations. This may include diversifying supply chains, implementing redundant systems, or establishing alternative work arrangements
- **Plan development**: Developing detailed business continuity plans BCPs that outline procedures and responsibilities for maintaining operations during a disruption. These plans should include communication protocols, resource allocation, and recovery steps
- **Training and awareness**: Educating employees about their roles and responsibilities in the event of a disruption. Regular training and awareness programs help ensure that staff are prepared to respond effectively
- **Testing and exercises**: Conducting regular tests and exercises to evaluate the effectiveness of business continuity plans. This helps identify gaps and areas for improvement, ensuring that plans are practical and actionable
- **Crisis management and communication**: Establishing a crisis management team to coordinate response efforts and communicate with stakeholders during a disruption. Effective communication is crucial for maintaining trust and transparency
- **Continuous improvement**: Regularly reviewing and updating business continuity plans to reflect changes in the organisation, emerging risks, and lessons learned from past incidents. Continuous improvement ensures that BCM remains relevant and effective.

  By implementing a robust Business Continuity Management framework, such as that illustrated within BS EN ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements[10], Public Sector organisations can enhance their resilience, minimise the impact of disruptions, ensure the ongoing delivery of critical services and operations, and maintain the trust of stakeholders.

  BS EN ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements provides a framework for organisations to plan, establish, implement, operate, monitor, review, maintain, and continually improve a documented management system to protect against, reduce the likelihood of, and ensure recovery from disruptive incidents.

# 7 Artificial Intelligence

Artificial intelligence (AI) involves creating machines that mimic human cognitive functions, enabling them to think and learn similarly to humans. This technology focuses on developing computer systems that can perform tasks usually requiring human intelligence, such as recognising speech, making decisions, solving problems, and translating languages.

AI is generally divided into two categories: narrow AI, which is designed for specific tasks, and general AI, which can comprehend, learn, and apply knowledge across various fields. Key AI technologies include machine learning, natural language processing, computer vision, and robotics.

The UK Government has published 'A Guide to Using Artificial Intelligence in the Public Sector'[11] highlighting AI's potential to transform public services by enhancing efficiency, decision-making, and service delivery. Some potential applications of AI in the public sector include:

- **Data Analysis and insights**: AI can process large datasets to uncover patterns, trends, and insights, aiding government agencies in making informed decisions, detecting fraud, predicting outcomes, and optimising resource allocation
- **Chatbots and virtual assistants**: AI-driven chatbots and virtual assistants can manage routine inquiries, provide information, and assist with transactions
- **Predictive analytics for public safety**: AI can analyse historical crime data, social media, and other relevant information to forecast crime hotspots, identify potential threats, and allocate resources effectively, thereby enhancing public safety and emergency response
- **Personalised services**: AI can tailor services by analysing individual preferences, behaviours, and needs, enabling customised recommendations, targeted communication, and service delivery
- **Automation of administrative tasks**: AI can automate repetitive tasks like data entry, document processing, and record keeping, saving time and resources
- **Healthcare and public health**: AI can aid in diagnosing diseases, predicting outbreaks, and improving healthcare delivery, thereby enhancing patient care and public health outcomes

Despite its benefits, AI also presents risks and challenges, as highlighted by Forbes[12]:

- **Job displacement**: AI could automate tasks currently performed by humans, leading to job losses and shifts in the job market
- **Bias and discrimination**: AI systems trained on biased data can perpetuate and amplify existing biases
- **Privacy and security concerns**: AI systems often require access to large amounts of personal data, raising privacy and data protection issues. Inadequately secured systems may be vulnerable to cyberattacks, leading to unauthorised access and misuse of sensitive information
- **Lack of transparency and accountability**: Some AI algorithms, like deep learning neural networks, are complex and difficult to interpret
- **Ethical considerations**: AI raises ethical issues, such as the potential for autonomous weapons, privacy invasion, and impacts on human autonomy and decision-making
- **Dependence and overreliance**: Excessive reliance on AI without proper human oversight can lead to errors or failures. Balancing AI capabilities with human judgment is crucial
- **Unemployment and socioeconomic inequality**: Widespread AI adoption could lead to significant job displacement, potentially worsening socioeconomic inequalities. Addressing these challenges through reskilling, upskilling programs, and social safety nets is essential

It is vital that any future regulations, standards, and ethical guidelines developed to ensure the responsible and beneficial use of AI technology are fully adhered to

# 8 Mould – Landlord Duties

In November 2022, a Coroner's Court examined the tragic death of a two-year-old child living in a property managed by Rochdale Boroughwide Housing[13]. This case drew national attention and underscored the urgent need for legislative action to hold landlords accountable for poor housing conditions. In response, the UK government published guidance on the health risks associated with damp and mould in September 2023[14].

Awaab's Law[15], set to be introduced in 2025, aims to address these issues by targeting social landlords, local councils, and housing associations. The law will be implemented in three phases:

- **Phase One** October 2025: Social landlords must investigate and resolve dangerous damp and mould issues within specified time limits, addressing emergency hazards within 24 hours
- **Phase Two** 2026: The scope expands to include hazards such as extreme temperatures, risks of falls, structural collapses, fire, electrical hazards, explosions, and hygiene concerns
- **Phase Three** 2027: This phase will cover all remaining hazards identified in the Housing Health and Safety Rating System England Regulations 2005[16]

**Legislation Overview**

Landlords, both private and social, must adhere to several legal standards to ensure tenant safety and avoid prosecution. Key legislation includes:

- **Housing Act 2004**[17]: Properties must be free from hazards, particularly 'category 1' hazards under the Housing Health and Safety Rating System HHSRS, which includes damp and mould
- **Environmental Protection Act 1990**[18]: Allows tenants and local councils to take legal action if homes are deemed a 'statutory nuisance,' posing health risks or being considered a nuisance
- **Landlord and Tenant Act 1985**[19]**, and Homes Fitness for Human Habitation Act 2018**[20]: Mandates properties to be hazard-free, including damp and mould, ensuring suitability for occupation

A home fit for human habitation is safe and healthy, free from damp and mould that could cause harm. Social housing must meet the **Decent Homes Standard**[21] (DHS), which requires properties to be free from hazardous 'category 1 conditions, adequately maintained, and provide thermal comfort. Failure to meet these standards can lead to enforcement actions by the Regulator of Social Housing.

Controlled work, such as heating and ventilation system repairs or window replacements, must comply with **Building Regulations**[22]. The Regulator of Social Housing updated its Consumer Standards[23] in February 2024, effective from April 2024, outlining obligations for registered providers of social housing. Regular inspections of larger landlords over 1,000 homes are part of the compliance program.

A Code of Practice[24] by the Regulator expects registered providers to conduct regular assessments of homes, ensuring they are safe, in good repair, and meet legal standards.

**Health Risks**

Mould poses significant health risks due to exposure to spores and mycotoxins[25]. Sensitive individuals, such as infants, the elderly, and those with allergies or asthma, may experience severe reactions. Moulds colonise water-damaged materials, secreting enzymes and producing toxins to compete with other microorganisms. Over 400 mycotoxins have been identified, causing symptoms like diarrhoea, headaches, skin irritation, fatigue, and compromised immunity, which can lead to opportunistic infections.

Black mould is particularly harmful, worsening breathing problems, infections, and allergies. It spreads across materials like paint, wallpaper, and plaster, often causing a musty smell. Excessive moisture and poor ventilation contribute to its growth, with condensation from everyday activities or structural defects being common sources.

**Landlords' Responsibilities**

Determining whether mould results from structural defects or tenant habits can be challenging. Landlords should inspect reported mould issues, make necessary repairs, and address any damage. Providing tenants with advice on preventing mould is beneficial.

**Tenants' Responsibilities**

Tenants also have responsibilities to prevent mould growth. They should ensure proper ventilation, maintain adequate heating, dry clothes outside, ventilate bathrooms and kitchens, keep furniture away from walls, use mould cleaners, and report damp or mould issues promptly.

**Summary**

Organisations should regularly review property maintenance to ensure tenant wellbeing. Tenants should be encouraged to adopt behaviours that prevent mould and report issues without delay. Prompt investigation and resolution of mould problems by landlords are crucial for maintaining safe and healthy living conditions.

# References


1. https://www.weforum.org/publications/global-risks-report-2024/
2. https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf
3. https://www.gov.uk/government/collections/local-government-reorganisation-policy-and-programme-updates
4. https://www.ncsc.gov.uk/
5. https://www.ncsc.gov.uk/cyberessentials/overview
6. https://www.weforum.org/publications/global-risks-report-2025/
7. https://www.nasa.gov/news-release/temperatures-rising-nasa-confirms-2024-warmest-year-on-record/
8. https://eos.com/blog/natural-disasters-2024/
9. https://www.bbc.co.uk/weather/articles/c1el8z2d7v8o
10. https://www.iso.org/standard/75106.html#amendment
11. https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector
12. https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/
13. https://www.bbc.com/news/uk-england-manchester-63635721
14. Understanding and addressing the health risks of damp and mould in the home. Available here: https://www.gov.uk/government/publications/damp-and-mould-understanding-and-addressing-the-health-risks-for-rented-housing-providers
15. https://www.housing.org.uk/resources/awaabs-law/
16. https://www.legislation.gov.uk/uksi/2005/3208/contents/made
17. https://www.legislation.gov.uk/ukpga/2004/34/contents
18. https://www.legislation.gov.uk/ukpga/1990/43/contents
19. https://www.legislation.gov.uk/ukpga/1985/70/contents
20. https://www.legislation.gov.uk/ukpga/2018/34/enacted
21. https://blog.goodlord.co/what-is-the-decent-homes-standard
22. https://www.gov.uk/guidance/building-regulations-and-approved-documents-index
23. https://www.gov.uk/government/consultations/consultation-on-the-consumer-standards/annex-3-consumer-standards
24. https://www.gov.uk/government/consultations/consultation-on-the-consumer-standards/annex-4-consumer-standards-code-of-practice
25. http://www.blackmould.me.uk/mould%20legislation.html

# Further Support

RMP Risk Control has a proven record in strengthening organisational risk and safety culture and lowering claims numbers and costs. By working in close partnership with our clients we raise and augment the profile of enterprise risk management across organisations.  Our team of qualified and experienced consultants based throughout the country have extensive experience of working closely with organisations, within the realms of health and safety, enterprise risk management, and fleet risk management to develop and deliver bespoke risk control programmes which are tailored to our clients' needs.

If you would like further information on any of our risk control services or to discuss your risk and safety needs, please contact your appointed RMP Risk Consultant, Ashley Easen - Director of Risk Consulting and ESG, or your appointed RMP Account Director.

Ashley Easen
Director – Risk Consulting and ESG

Tel: (+44) 07825 365090

ashley_easen@gbtpa.com

www.gallagherbassett.co.uk

On occasion, RMP Risk Control will deliver services via our extended network of approved Associate Consultants. These consultants have successfully passed our stringent vetting processes, and their use will be agreed with our clients prior to project initiation.

**Risk Management Partners**

67 Lombard Street
London EC3V 9LJ
020 7204 1800
contact@rmpartners.co.uk

**rmpartners.co.uk**

Visit our website and find out more facts about the Public Sector:
rmpartners.co.uk

Dedication in action



FP497-2025