XL Insurance

Navigating AI Complexity: Robust Strategies for Operational Resilience

Sustaining Service and Resilience

Ayse Aksay
Head of Risk Governance, Control and Operational Risk, AXA XL

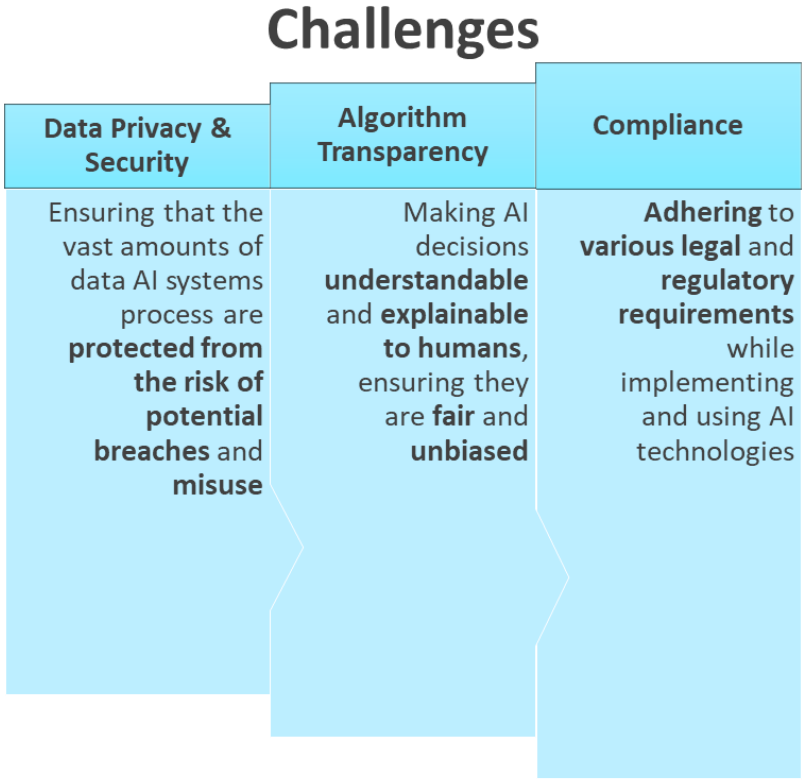
Artificial Intelligence (AI) in Financial Services

- AI is revolutionising financial services, bringing both innovation and new challenges
- Keeping services running smoothly is vital for client and employee protection
- Managing AI risks is crucial to protect the business and ensure smooth operations
- Manage AI complexity with robust governance, enhanced infrastructure, and ongoing collaboration and training

Understanding AI complexity

- **Integrating AI into existing systems** involves processing massive amounts of data, creating sophisticated algorithms, and ensuring seamless **interaction with other technologies**

- AI systems are composed of **multiple components**, including **data collection**, **machine learning models**, and **decision-making processes,** each **adding a layer of complexity**



Threats to Operational Resilience

System Failures

AI systems can sometimes break down or malfunction

Cybersecurity Vulnerabilities

AI systems can be targeted by hackers, making them vulnerable to cyber-attacks. Hackers might exploit weaknesses in an AI system used for online services, potentially stealing sensitive customer and/or employee information

Bias in AI Decisions

AI systems can sometimes make unfair or biased decisions, which can affect service quality and client/ employee trust

Data Breaches

Large amounts of data are processed by AI systems, which can be at risk of being breached or misused. A data breach in an AI system used for customer analytics could expose personal information, leading to privacy violations

AI-related errors, cyber-attacks, system failures, and non-compliance with regulations can lead to significant financial losses, reputational damage, and legal penalties for businesses

Infrastructure and Defenses

Protecting the Business

Risk Management Framework

1) Impact of AI on the Risk Management Framework

- Integrate risks related to AI, such as data privacy, algorithmic errors, and cyber threats, into the overall risk management strategy
- Create policies and governance specifically addressing AI risks
- Regularly identify and assess potential AI-related risks
- Develop and implement mitigation strategies for identified AI risks

Infrastructure Defences

1) Cybersecurity Measures 2) Regular Updates & Checks 3) Data Protection Methods

- Use next-gen firewalls and intrusion detection systems to monitor and block unauthorised access
- Require Multi Factor Authentication (MFA) for accessing sensitive AI systems and data
- Regularly update AI software to patch vulnerabilities and improve functionality
- Use automated tools to continuously monitor AI systems for any unusual activity or signs of malfunction
- Encrypt sensitive data both at rest and in transit to prevent unauthorised access
- Implement strict access controls to limit who can view or modify data

Audits, Control Testing and Risk Assessment

1) Continuous Monitoring for Sustainability

- Regularly monitor AI systems to ensure they comply with regulations and perform as expected
- Perform stress tests to evaluate how AI systems perform under extreme conditions
- Regularly conduct vulnerability assessments to identify potential security gaps and address them promptly

Agile Strategies for Operational Resilience

Agility in Risk Management	Robust Strategies	Training and Awareness Programmes
○ *Quick Response to AI-Related Issues*	○ *Continuous Monitoring and Adjustment* ○ *Scenario Planning for AI-Related Incidents* ○ *Education on AI Risk Management and Response*	○ *Regular Training on AI Risks* ○ *Encourage Teamwork to Improve Resilience*
• **Incident Response Teams**: Establish dedicated teams trained to handle AI system failures or breaches immediately • **Automated Alerts**: Use AI to set up real-time monitoring and automated alerts to identify and respond to issues quickly	• **Performance Metrics**: Track key performance indicators (KPIs) to assess AI system health and identify areas for improvement • **Adaptive Algorithms**: Implement AI algorithms that learn and adapt over time to new data and threats • **Risk Scenarios**: Develop and simulate scenarios such as AI system failures, data breaches, and algorithmic biases • **Response Plans**: Create detailed response plans for each scenario, outlining steps to mitigate impacts and restore operations • **Regular Workshops**: Conduct workshops and training sessions focused on AI risk management and response • **Simulation Exercises**: Use simulation exercises to practice responding to AI-related incidents	• **Online Courses:** Provide access to online courses and resources on AI and risk management • **Expert Sessions:** Invite AI and risk management experts to share insights and best practices • **Cross-Functional Teams**: Form cross-functional teams involving IT, risk management, compliance, and business units to address AI risks comprehensively • **Regular Meetings:** Schedule regular meetings to discuss AI risk management strategies and share updates

Leveraging AI for Enhanced Risk Monitoring

AI enhances business operations by enabling early threat detection, improving decision-making with data-driven insights, and accurately predicting future risks for proactive planning and compliance

Some strategies to manage AI complexity effectively

Emerging Trends in AI

1)AI and Quantum Computing

- Quantum computing is set to revolutionise AI by significantly speeding up data processing and solving complex problems faster than traditional computers

2)AI Ethics and Responsible AI

- Growing focus on ethical AI use, ensuring fairness, transparency, and accountability in AI decision-making

3) AI and Personalisation

- Enhanced personalisation in financial services, providing tailored experiences and products to customers based on AI-driven insights

4) AI in Cybersecurity

- Advanced AI-driven cybersecurity measures to predict and prevent cyber threats more effectively

5) AI Regulation and Compliance

- Anticipating new regulations specifically targeting AI, requiring businesses to adapt their compliance strategies

Key Takeaways

- AI adds layers of complexity to financial services, including integration and decision-making challenges
- Ensuring continuous operation of critical services is essential amidst AI-driven complexities
- Effective AI risk management includes robust governance, strong cybersecurity, and continuous monitoring
- Be ready to quickly respond to AI-related issues with adaptive and agile strategies
- Use AI for enhanced risk monitoring, early threat detection, and informed decision-making
- Stay ahead of emerging AI trends and their impact on financial services for proactive planning and compliance

Thank you

Know You Can