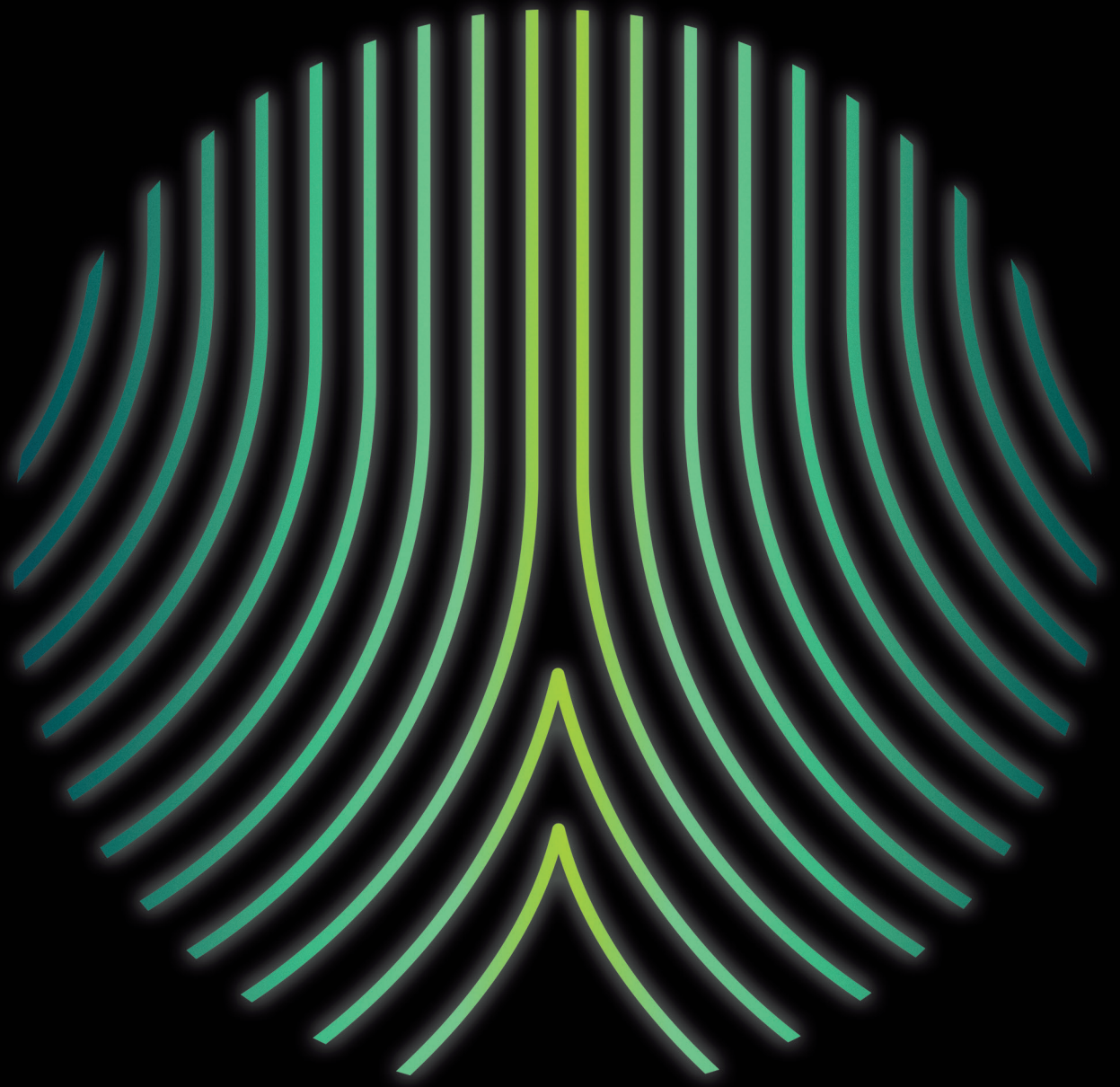
Deloitte.



Algorithm Assurance

Ensuring algorithms are working as intended

Deloitte Malta

Audit & Assurance

What is algorithm assurance?

In computer science and mathematics, an algorithm is a set of computer statements designed to perform complex calculations or problem-solving operations.

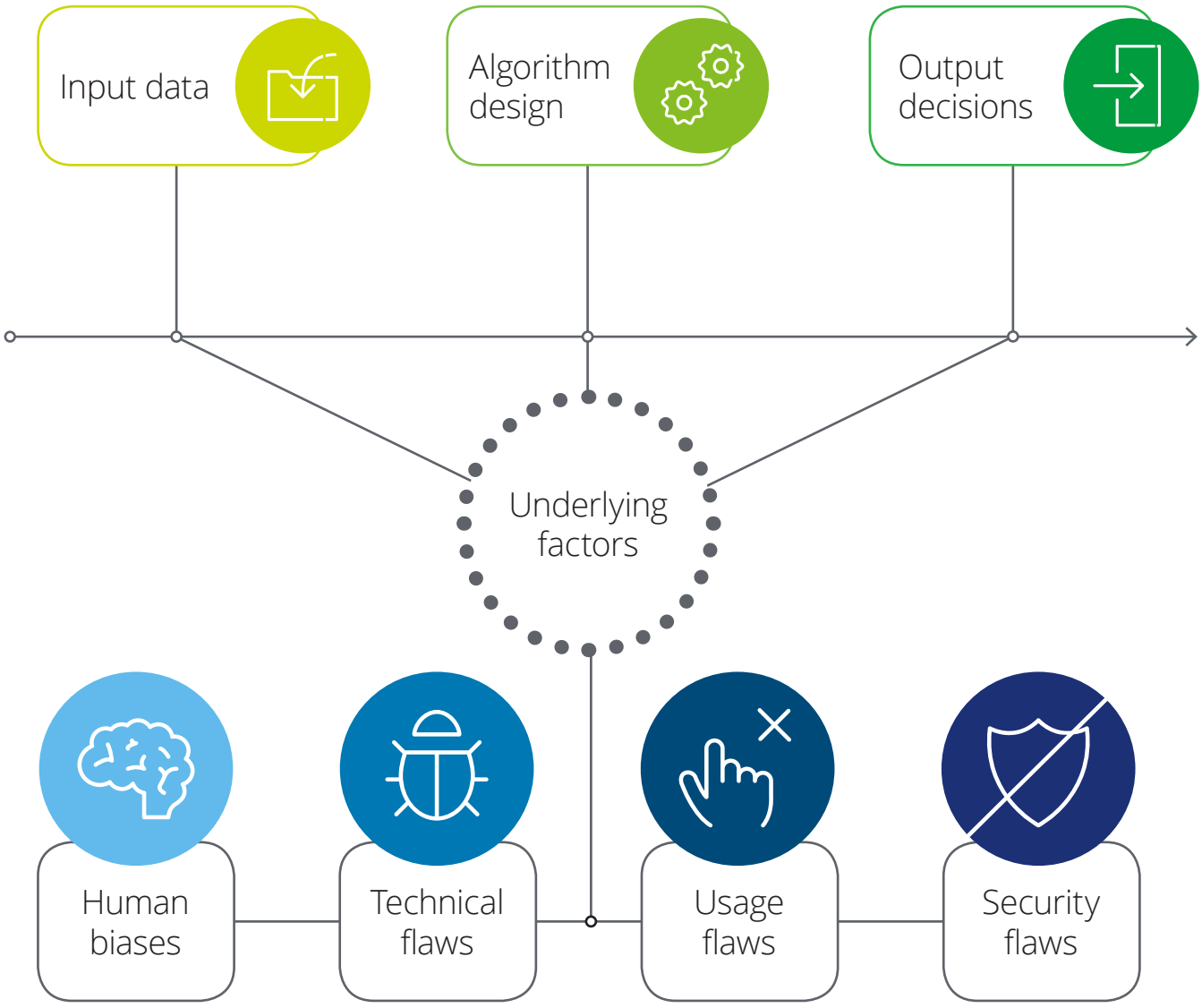
Algorithm assurance is the process which tests whether those statements are conforming to their intended design goals and achieving the desired outcomes.

Algorithms are not new tools - the world's first algorithm for an early computing machine, which only existed on paper, was developed by Ada Lovelace in the 1840s. Nowadays the capabilities, prevalence and complexity of algorithms has evolved and there are a myriad of algorithm designs that are tailored to address specific problems. Algorithms are used extensively in different market sectors. For example:

- Machine learning algorithms are used in the health care industry to identify cancerous tumours;
- Neural networks algorithms are used by businesses to aid in sales forecasting, customer profiling and data validation;
- Pattern recognition algorithms are used in speed cameras to identify overspeeding vehicles;
- Predictive systems are used to provide a best assessment of the likelihood of future outcomes on statistical and historical data; and
- Rules-based algorithms are used in the wholesale financial markets to automatically determine order initiation, generation, routing or execution on an exchange, without human intervention.

The use of intelligent algorithms offers a wide range of potential benefits to organisations. However, algorithms also have the potential to produce unexpected and unintended results, and the risks of algorithms malfunctioning therefore have wide-ranging consequences for all stakeholders. The effects of ill-designed algorithms could result in financial losses, harming firms' reputations, regulatory implications, severe disruptions to operations and (in extreme instances) could also result in the loss of human life. The activities handled by algorithms typically occur at great speed, which means that existing risks could be amplified if risk management and other controls are not effective[1].

Framework for understanding algorithmic risks



Algorithm risks

Algorithmic risks arise from the use of data analytics and cognitive technology-based software algorithms in various automated and semi-automated decision-making environments.

Deloitte US has developed a framework for understanding the different areas that are vulnerable to such risks and the underlying factors causing them.

- Input data is vulnerable to risks, such as biases in the data used for training; incomplete, outdated, or irrelevant data; insufficiently large and diverse sample size; inappropriate data collection techniques; and a mismatch between the data used for training the algorithm and the actual input data during operations[2].
- Algorithm design is vulnerable to risks, such as biased logic: flawed assumptions or judgments; inappropriate modelling techniques; coding errors; and identifying spurious patterns in the training data[2].
- Output decisions are vulnerable to risks, such as incorrect interpretation of the output; inappropriate use of the output; and disregard of the underlying assumptions[2].

The risks around input data, algorithm design and output decisions can be caused by several underlying factors:

Human biases: *Cognitive biases of model developers or users can result in flawed output. In addition, lack of governance and misalignment between the organisation's values and individual employees' behaviour can yield unintended outcomes. Example: developers provide biased historical data to train an image recognition algorithm, resulting in the algorithm being unable to correctly recognise minorities.*

Technical flaws: *Lack of technical rigour or conceptual soundness in the development, training, testing, or validation of the algorithm can lead to an incorrect output. Example: Bugs in trading algorithms drive erratic trading of shares and sudden fluctuations in prices, resulting in millions of dollars in losses in a matter of minutes.*

Usage flaws: *Flaws in the implementation of an algorithm, its integration with operations, or its use by end users can lead to inappropriate decision making. Example: Drivers over-rely on driver assistance features in modern cars, believing them to be capable of completely autonomous operation, which can result in traffic accidents.*

Security flaws: *Internal or external threat actors can gain access to input data, algorithm design, or its output and manipulate them to introduce deliberately flawed outcomes. Example: By intentionally feeding incorrect data into a self-learning facial recognition algorithm, attackers are able to impersonate victims via biometric authentication systems.*

The above factors are sourced from: Deloitte US, "Managing algorithmic risks" 2017. See references at end for details.

Algorithm regulation

The algorithm's internal complex operations appear as "black boxes" to those on the outside world[3] and consequently the resultant output raises concerns about the inherent trust attributes. As our lives are becoming more and more affected by algorithms outputs, there has been a surge of global regulatory activity and regulators are initiating greater scrutiny on firms to ensure proper compliance with the regulations and instil trust in algorithms outputs.

In certain jurisdictions, similar to the audited financial statements requirement, there is a requirement that algorithms also undergo a degree of review and where independent auditors are hired to provide the necessary assurance.

MiFID II (a legislative framework instituted by the European Union to regulate financial markets in the bloc) Regulatory Technical Standard 6 (RTS 6), specifies the organisational requirements of investment firms engaged in algorithmic trading. More precisely, the standard details the requirement for all investment firms that offer direct electronic access (DEA) for clients and/or perform algorithmic trading to undertake annual self-assessments to ensure continued compliance with RTS 6[4]. In order to make algorithmic trading self-assessment defensible in front of regulators, firms have had to strengthen their control framework across the three lines of defence focusing on five thematic areas: governance, testing and deployment, algorithm controls, monitoring and documentation.

In its strive to become one of the leaders in the digital world, Malta recognises the importance of regulation as one of the pillars that enables trust and facilitates the adoption of new technologies. Regulatory frameworks for remote gaming, financial services and blockchain are flourishing on the island and have created new economic niches. The next logical step was the exploration of algorithms, particularly in the field of Artificial Intelligence (AI), whereby, in support of the 'Strategy and Vision for AI in Malta 2030' and the achievement of the Malta Ethical AI Framework, the Malta Digital Innovation Authority (MDIA) is in the process of expanding the Innovative Technology Arrangements (ITA) certification framework for AI-based solutions5. The AI certification programme purports to ensure that the underlying AI algorithms are developed in an ethically aligned, transparent and socially responsible manner. Central to this programme is the Systems Audit which is a reasonable assurance engagement that includes the assessment of common criteria defined by the MDIA such as availability, processing integrity, confidentiality, risk management and design and implementation of controls, monitoring of controls, change management and functionality and compliance with regulatory requirements.

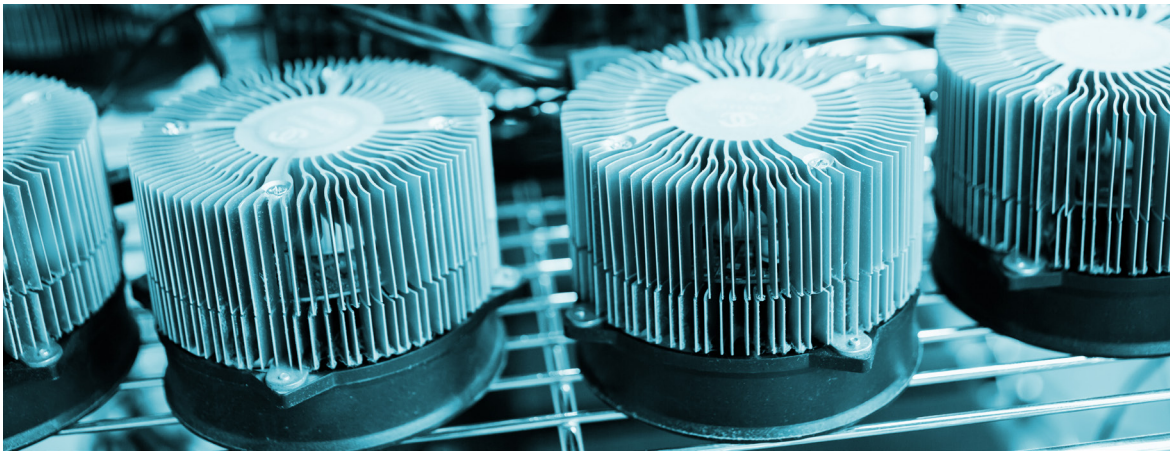
Algorithm control framework

Because the area of algorithm assurance is relatively new, regulations and guidelines are still evolving, creating a challenging algorithmic accountability, transparency and compliance landscape6. Algorithm assurance goes beyond code review (reading through the algorithm source code, or pseudo code, to identify potential errors or vulnerabilities); and a robust algorithm control framework is fundamental to algorithm risk management. The framework should cover key areas including governance and oversight, algorithm pre and post go live testing, specific algorithm controls around key risk, monitoring, surveillance and appropriate levels of documentation[6]
.
Increasing complexity and lack of transparency, around algorithm design, inappropriate use of algorithms and weak governance are specific reasons why algorithms are subject to such risks as biases, errors, and malicious acts. Consequently, algorithmic risk management cannot be a periodic point in time exercise and requires continuous monitoring[2].

Adopting the International Standard on Assurance Engagements ISAE 3000, for the purpose of providing assurance over the operational effectiveness of algorithms and their associated controls, is crucial in providing assurance that the algorithm control framework meets the current, relevant and defined standards, and that it has operated effectively within the period under review.

Adequate assessment of the algorithm risks at the input, design and output layers and the surrounding control framework should help the auditor performing algorithm assurance to formulate an opinion on the suitability, reliability of the controls around and embedded in the algorithm.

The tasks performed during algorithm assurance engagements naturally rest within the realm of IT auditing. Notwithstanding, assistance from specialist interdisciplinary teams is required to understand and manage the risks emerging from the use of algorithms. Algorithm assurance should also integrate professional scepticism with social science methodology and concepts from such fields as psychology, behavioural economics, human-centred design, and ethics[3].



Conclusion

In a world where algorithms are more prevalent, with increased volumes of data, processes automation and decisions being made by algorithms, the need is greater for assurance that the underlying algorithms are working as intended and achieving the desired outcomes[7]. Algorithm assurance is one way for stakeholders, organisations and regulators alike to gain trust in algorithms performing complex decisions and to how well the related risks are being managed and controlled.

In response to the exponential use of algorithms, different regulatory regimes are demanding the requirement of an independent algorithm assurance engagement. Although these engagements can be regarded as additional and avoidable operational costs; if well executed, algorithm assurance can potentially identify weaknesses in the underlying algorithm control framework, which if not managed properly can expose the related firm to different algorithm risks that may lead to catastrophic consequences.

Ultimately, managing algorithm risks and complexities can be an opportunity to lead, navigate and disrupt in industries and functions[2].

References

1. Prudential Regulatory Authority, "Consultation Paper | CP5/18 - Algorithmic trading" February 2018
   https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2018/cp518
2. Deloitte US, "Managing algorithmic risks" 2017
   https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-algorithmic-machine-learning-risk-management.pdf
3. Harvard Business Review, "Why We Need to Audit Algorithms?" November 2018
   https://hbr.org/2018/11/why-we-need-to-audit-algorithms
4. Deloitte UK, "MiFID II RTS 6 Requirements: Annual Self-Assessment" May 2019
   https://blogs.deloitte.co.uk/assurance/2019/05/mifid-ii-rts-6-requirements-annual-self-assessment-guiding-your-firm-through-uncertainty.html
5. [5] MDIA "AI ITA Guidelines" October 2019
   https://mdia.gov.mt/wp-content/uploads/2019/10/AI-ITA-Guidelines-03OCT19.pdf
6. Deloitte UK, "Algorithm Assurance" 2019
   https://www2.deloitte.com/uk/en/pages/audit/solutions/algorithm-assurance.html
7. Deloitte Australia, "Assurance over machine learning and algorithms". March 2018
   https://www2.deloitte.com/au/en/pages/audit/articles/assurance-over-machine-learning-algorithms.html#

Please contact Deloitte Malta Audit & Assurance for more information:

Sandro Psaila
IT Audit & Assurance Senior Manager
spsaila@deloitte.com.mt

David Delicata
Assurance Leader
ddelicata@deloitte.com.mt

Deloitte
Deloitte Place
Mriehel Bypass
BKR 3000, Malta

Tel:+356 2343 2000

www.deloitte.com/mt/assurance

Deloitte.