Deloitte.

# Augmenting trade surveillance programs with artificial intelligence and machine learning: A brief overview

**May 2024**

MAKING AN IMPACT THAT MATTERS since 1845

"What we were looking to do here was really to answer some of the questions that were presented in surveillance: changing market conditions, increased volatility, increased volumes and change in conduct. And so, using deep learning made a lot of sense to start to answer those challenges."

—Susan Tibbs, Former Vice President, Market Manipulation Group, Financial Industry Regulatory Authority (FINRA)[1]

PRINTING INSTRUCTIONS

# Artificial intelligence: A brief overview

The financial markets have generally been a hotbed of competitiveness, risk, and innovation. To uphold the economy's good health and to build investor confidence, it is crucial to maintain integrity and stability of financial markets. In this world of fast-paced technological developments, artificial intelligence (AI) is becoming a potent weapon in the field of risk monitoring and surveillance. By looking at its diverse applications and upcoming trends, AI may be a crucial factor in helping to protect financial markets.

AI involves the use of algorithms and analytics to enable systems to demonstrate intelligent behavior, including learning from data, making decisions, and solving problems, all with minimal human intervention. Similarly, machine learning (ML) is the process of discovering patterns in data without human intervention and using them to make predictions. Specific to trade surveillance, systems integrated with AI and ML not only aim to uncover suspicious trading patterns, but also to help in reducing the volume of false alerts, thereby helping mitigate their risk to the trading ecosystem.

With AI being considered as a key element in future innovations, the financial services industry is looking to leverage its potential as a transformative tool. In areas such as improved fraud detection, risk management, and predictive analytics.[2] Some common AI use cases in the banking and financial services sector include:

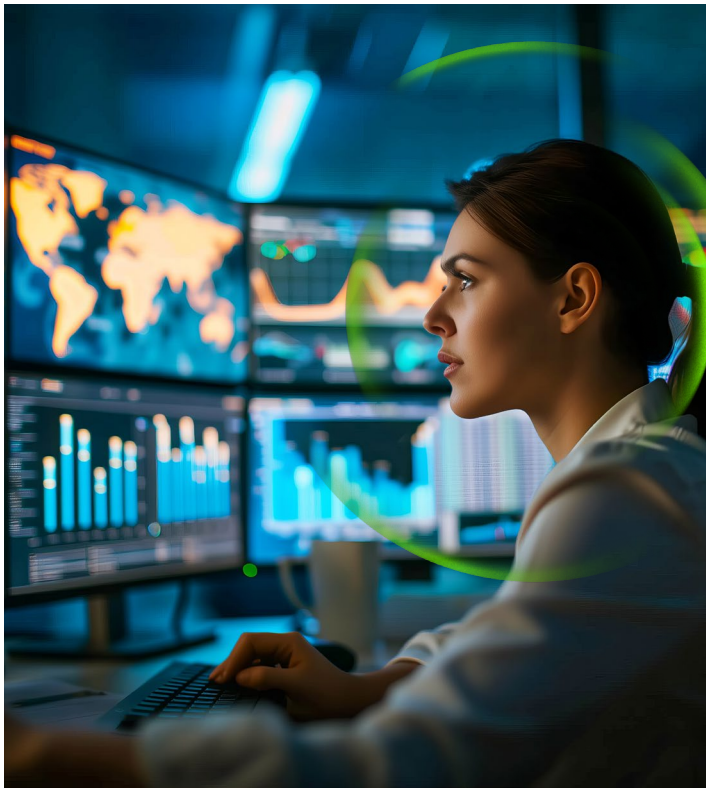

# Rule-based surveillance: Status quo

Market surveillance has traditionally been rule-based, generating alerts based on pre-specified rules/static thresholds that lead to specific actions when such conditions are breached. Due to high interpretability, these "traditional" surveillances have the main advantage of being simple and reliable, meaning they are easier to understand and develop/enhance standardized rules that would enable ongoing market surveillance. However, while rule-based systems have been quite effective in laying a successful foundation for trade surveillance, they have limitations due to them not being effective for all use cases:

- **Data cleansing requirements:** Rule-based systems often struggle with large and unstructured datasets that require extensive efforts in cleansing and formatting to make it well-structured and usable for surveillance systems.
- **Tackling new threats:** Rule-based systems work based on prescribed/preconditioned directives; hence they cannot pick up manipulative patterns that are new or even slightly modified, resulting in possible surveillance lapses.
- **Adaptability across markets:** Rule-based systems require dedicated models to cover different asset classes and markets. While these systems currently have dynamic thresholds that may help to an extent, they still need to account for manageability, as firms may end up with a significant number of models and an even higher number of thresholds/parameters across asset classes and markets that require a larger maintenance effort, making this construct susceptible to errors.

To tackle the limitations and challenges of rule-based surveillance, there is widespread consensus among market participants and regulators about the need to analyze more dynamic and robust surveillance insights for the future[3] AI and ML models are being considered by both regulatory authorities and financial institutions (FIs) as an accelerator for market surveillance. Alternative solutions are also being explored in parallel for enhancing existing surveillance capabilities as well:

- **Quantum computing** is being looked at as a potential accelerator for AI as it could enhance the ability of AI-based models to process and analyze large datasets at faster speeds.[4]
- **Network and behavioral analysis** techniques could help in revealing hidden connections/relationships/patterns to identify potential coordinated market manipulation behaviors. Deviations from normal behavior patterns could result in identifying evidence of market abuse.



- **Holistic surveillance** is an approach that enables simultaneous monitoring across multiple surveillance functions, supporting higher-quality tethering and control effectiveness between trade and communications data to help identify false or misleading statements and potential market abuse behaviors such as "pump and dump," "flying," and "printing".[5]
- **Dynamic parameters** can be used to determine and assess specific trading behaviors more accurately based on factors like the standard deviation of client or account trading activities/patterns, market conditions, and economic indicators when compared to static thresholds. This approach can help diminish the number of false positives, which has been a significant drawback of rule-based surveillances.
- **Integration of distributed ledger technology (DLT)/blockchain with AI** at the back end for data storage and retrieval could help tackle the opaque nature of AI. The immutability, traceability, and decentralized nature of DLT/blockchain enables improved security, transparency of execution, and efficiency that could be a strong fit for AI-based surveillance systems.

# Rule-based surveillance: Status quo (cont.)

In addition to the above areas, many FIs are looking at AI and ML as an augmentative solution for trade surveillance. Integration of AI/ML in existing surveillances has the potential to be a great value add for organizations looking to enhance surveillance efficiency and overcome the limitations posed by traditional surveillance analytics. Some of the benefits AI can provide around surveillance include:

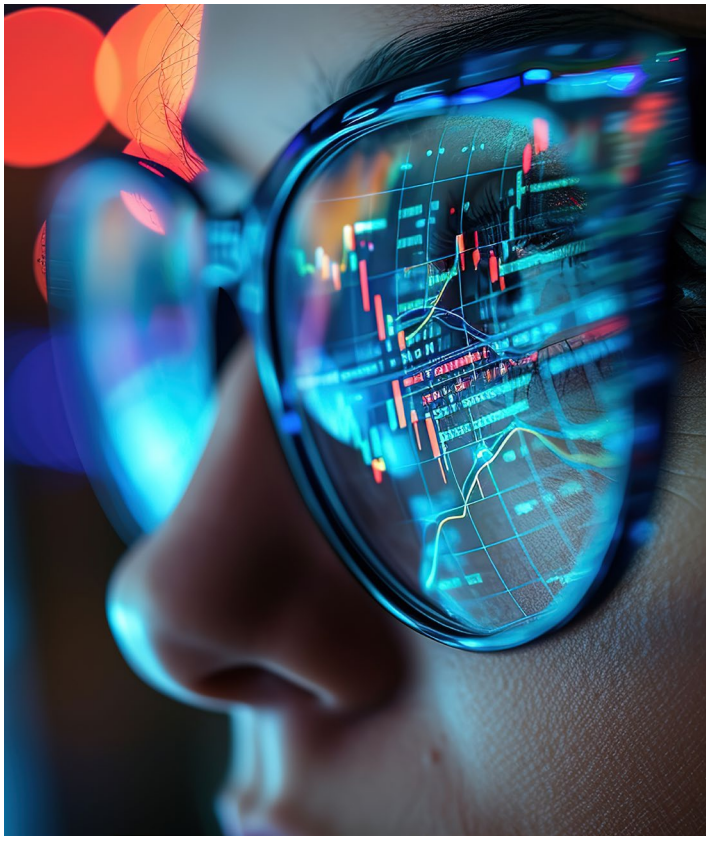
- **Adaptive and scalable surveillances:** AI-based models are capable of processing large datasets quickly and highlight evolving patterns of potential market manipulation-related activities. The capability of AI-based models to process large and diverse datasets could assist firms to identify and manage risk more appropriately. ML models stand out in handling uncertainties as they can provide confidence scores, or probabilities associated with their predictions, which is valuable when dealing with varied trading and order placement behaviors. The personalization feature of AI/ML makes it possible to create alerts that are more pertinent and in line with the distinctive market dynamics of various financial instruments. Based on their risk appetites and trading methodologies, AI allows organizations to customize alert thresholds. For example, with the help of AI/ML models, dynamic thresholds/parameters can be set for a variety of clients. Clients with low turnover/trading activity and trading manually can be distinguished from clients trading in large volume and on low-latency/high-frequency flows using complex trading algorithms. With the help of AI, a clear distinction can be made while generating alerts for such activities.
- **Reduction of false positives:** A major concern with rule-based systems is increasing alert volume and the time involved in reviewing the same. Integration of AI in trade surveillance can help to reduce false positives and alerts posing no risk, and increase learnability and feedback loops with historical market and surveillance data.
- **Real-time identification of patterns and anomalies:** AI-enhanced models can identify patterns in trading activities and relate them to generic or specific market events that may indicate trading anomalies. For instance, AI-integrated surveillance models designed to detect intraday market manipulation risk can identify market volatility resulting from index rebalancing, option expiry events, or movement in a stock's price because of issuer-specific news and compare outcomes to historic situations to more effectively trigger or provide supporting information. This can increase the effectiveness of models to proactively trigger alerts on unusual participation or movements in price that may not be attributed to any specific external events. The model can also aid in spotting trends and abnormalities, including ones that rule-based systems might miss, to recognize complex patterns that may not be immediately evident.
- **Supporting the surveillance review:** The integration of AI in surveillance can enhance the surveillance review process, making it more efficient and effective. By leveraging e-discovery usecases, electronic communications can be reviewed with greater ease and accuracy. For instance, a four-month review that required one million documents and a hundred personnel was reduced to six weeks and five personnel by utilizing large language models with search prompts. This technology enables analysts to identify the origin of trades and patterns of behavior beyond traditional rule-based surveillance, thereby enhancing the overall surveillance experience.[6]

# Feasibility of implementing AI in surveillance

Trade surveillance requires data from multiple sources including but not limited to exchanges, venues, trading platforms, news feeds, and internal trading records. Accessing and integrating data from these diverse sources can be technically complex. When combined with surveillance data from communications, it can lead to a more efficient and effective analysis and interpretation of suspicious activity. This approach recognizes that different AI models may excel in different aspects of surveillance and combining their strengths can lead to more robust results. Various stand-alone models can be configured and trained for specific aspects of surveillance. Implementing AI comes with specific requirements and prerequisites that are essential for its successful adoption.

- **Natural language processing (NLP)** models for speech-to-text data, translation engines, analyzing news, sentiment, and textual data related to financial markets.
- **Time-series models** like recurrent neural networks (RNNs) or long short-term memory (LSTM) networks for detecting patterns and trends in historical trade data and behavior.
- **Graph-based models** to analyze the relationships and connections among different entities in the financial markets, such as traders, firms, and securities.
- **Anomaly detection models** to flag unusual trading behavior.

It is vital to define clear objectives and use cases for AI in both trade and communications surveillance. Whether related to risk appetite of the entities or driven by rules, guidance, or mandates from regulators and venues, having specific goals can aid in greater effectiveness of an AI-based model. It is essential to have appropriate infrastructure in place. This includes the hardware and software needed to collect, store, and process data efficiently. High-performance servers, data management tools, and storage solutions are required for handling the vast amounts of data involved across surveillance purposes. Access to a substantial amount of historical data is essential to train a robust and accurate model. This helps the AI system learn from past events and identify patterns of misconduct. Sufficient education across technology, compliance, and surveillance teams enables the effective use and feedback loops to improve the effectiveness and efficacy of integrating AI into surveillance systems.



Once the technical infrastructure for AI implementation is in place, human expertise should be leveraged to add maximum value to the efficiency of the AI-based model. Right from the thoroughness of data till the end results, human skills are pivotal to choose the appropriate inputs. If the model produces below-par results, the model owner is held responsible since they make all the important decisions pertaining to developing, training, and maintaining AI models. The organization's commitment to meet these foundational requirements are important for the success of the AI implementation.

# Opaque nature of AI


With the use of AI in surveillance, there may be a tendency to be wary of its opaque nature and lack of transparency of underlying algorithms—how the model operates (its dependencies and limitations) and how its predictions or results are produced. This closed approach surrounding AI makes it challenging for a non-technical audience to understand the model logic. To address this inherent skepticism, firms can:

- **Document** the design, purpose, and key features of the model to make clear the inputs and expected outputs.
- **Build dashboards and visuals** to explain the flow of model decision-making and, subsequently, provide detailed explanations of alert predictions.
- **Assess data quality** to provide confidence in the design and operation of models used. This may include using exploratory data analysis as well as sandbox environments with both true-positive and false-positive examples, back-tested data, and stress-tested environments.
- **Implement controls below the line** and periodic review of results to provide confidence in inputs and outputs.

This can help to reduce ambiguity surrounding the opaque nature of AI, and organizational personnel can get comfortable with AI's capabilities to make consequential compliance decisions.

# AI/ML in surveillance: The regulatory perspective

The banking and financial services sector is highly regulated, constantly trying to uphold its fundamental value of data governance/protection and customer privacy.[7] However, increasing adoption of AI and ML can pose a distinct challenge regarding model explainability.

ML models often provide for some explainability in terms of the underlying assumptions and factors considered when making a prediction. The regulators recommend improving explainability of the AI/ML model being used to help users and supervisors understand the functionality by breaking down the opaque nature to provide clarity.[8] To tackle the challenges stated above, establishing a trustworthy AI framework that helps organizations develop ethical safeguards to address key concerns across the following dimensions is crucial in managing the risks and capitalizing on the returns associated with AI:

- **User privacy** – Implementing controls to ensure data usage is limited to its intended and stated use and duration, with users having the option to share data.
- **Transparency and explainability** – Tackling the opaque nature of AI to ensure that users understand how the AI/ML models work by explaining the inputs, inherent logic involved in decision-making and outputs such that the decision-making is clearly understood, auditable, and open to inspection.
- **Accountability** – Ensuring policies are in place to determine responsibility and ownership of decisions made by the AI/ML models.
- **Safety and security** – Ensuring controls are in place to protect the AI/ML models from risks that could have a significant negative impact on the firm/stakeholders.
- **Reliability and robustness** – Implementing controls to ensure accurate outputs, withstand errors, and quickly recovery from unforeseen disruptions.

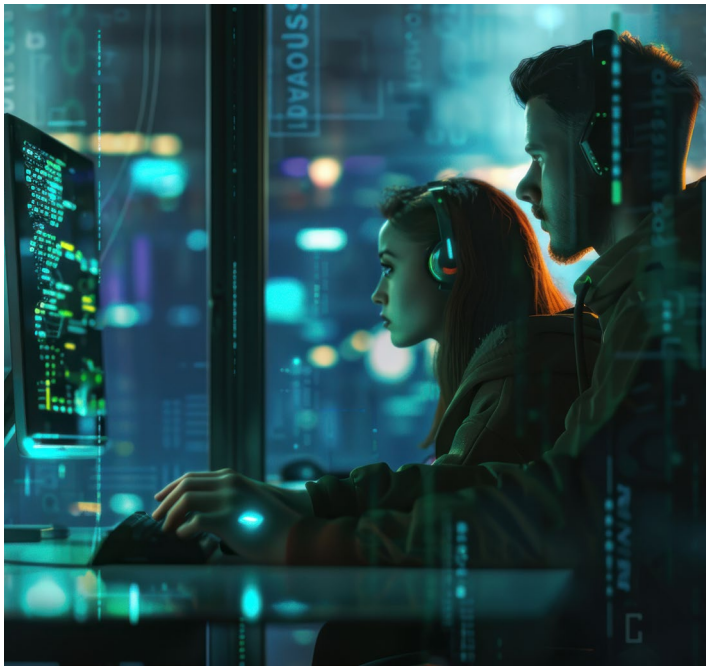
At Deloitte, we provide an end-to-end framework to assist with the implementation of AI that echoes the application of all the above-stated dimensions to build an ethically adept AI/ML system. Please refer to Deloitte's Trustworthy AI™ framework to learn more.

# AI/ML in surveillance: Technical standpoint

An AI-implemented surveillance solution is considered effective if it is proficient in recognizing trading patterns. Market manipulation patterns can be recognized through a combination of data analysis, pattern recognition algorithms, and machine learning techniques. Prior to analysis, relevant trading data is sourced and prepared for pre-processing and feature extraction. AI algorithms are used to identify patterns within the pre-processed data–these could be trend-based, reversal-based, or other trading pattern types used to detect anomalous trading behavior. Supervised and unsupervised learning approaches are used to train ML models so that trading outcomes are more closely correlated to input features. Techniques such as clustering, dimensionality reduction, time series analysis, and deep learning can be leveraged in pattern identification (deep learning is a method in AI that teaches computers to process data in a way that is inspired by the human brain). Identified trading patterns are reviewed via model evaluation, back testing, and validation including manual analysis wherever necessary. Since market dynamics are ever changing, the nature of market manipulation patterns needs to be evaluated on an ongoing basis, so that AI-based surveillance models keep performing effectively.

ML models score alerts, not only based on the data points directly related to the alert (e.g., parameter or threshold breaches of volumes or prices), but also on how similar alerts have been classified by the firm's risk and compliance division previously. AI-based alert scoring is particularly useful when alerts are generated through a traditional rule-based approach. This is because the scoring functionality can be considered as a second layer, which is implemented on top of the regular alert-generating process and, as such, can also optimize the outcome of legacy trade surveillance systems.

Being an area with vast potential and a steep learning curve, experienced practitioners of AI in surveillance are in short supply. Developing an understanding of AI concepts and techniques requires sound knowledge of data analysis, feature extraction, and anomaly detection. Additionally, having working knowledge of econometrics (regression, time series analysis, etc.) and ML helps to develop clearer concepts of AI model development, testing, validation, and governance. For implementing AI in



surveillance, practitioners should have a strong grip on market abuse/manipulation processes, models, and regulations so that business requirements and technical specifications are aligned. It should be noted that AI is still a developing area, hence knowledge of technologies and concepts needs to be updated on an ongoing basis.

There are multiple benefits in leveraging AI in the surveillance world; however, having skilled resources to implement AI is essential. A group of professionals well-versed in AI technologies and concepts are more likely to effectively bring AI into practice. In this regard, surveillance professionals still have some way to go in being AI proficient and are currently dependent on technical specialists for AI implementation. To bridge this gap, training on AI concepts and use cases can help traditional surveillance professionals become more familiar with onboarding AI solutions.

# Conclusion and key takeaways

Financial institutions can focus on developing and improving surveillance models as an integral part of their journey to establish an extensive surveillance program. A well-defined and understood risk framework serves as the scaffolding to construct and operationalize a trustworthy AI program. Once the risk models to be covered under the surveillance program are decided, the risk and compliance team can evaluate which alert models can benefit from implementation of AI. AI can be used to either create a new surveillance model, adjust an existing one, or improve rule-based and static surveillance models. It may not always be beneficial to develop AI into simple rule-based surveillances like potential wash trading and locates. Also, AI should not be incorporated into surveillance programs of small firms with manageable trading volumes as it would not have a drastic impact on efficiency or effectiveness compared to existing off-the-shelf products. However, large firms dealing with significant trade, order, and communications data; using complex trading mechanisms; and having sophisticated clients will likely benefit more from implementing AI into their existing surveillance programs.

As stated earlier, building and implementing an AI framework with governance and regulatory safeguards across key dimensions such as data privacy, accountability, and reliability is a crucial step in managing the risks and capitalizing on the returns associated with artificial intelligence. Please refer to Deloitte's Trustworthy AI™ framework to learn more about our end-to-end framework to help synergize ethical AI implementation and integration with organizations.

Organizations should view the implementation of AI in surveillance as an evolving and an ongoing process; while AI may require resources like technology, infrastructure, and skilled human capital, learning, testing, enhancing, and iterating needs to happen on an ongoing basis to be successful. This can be achieved with the help of a dedicated AI center of excellence (CoE) within the organization. Institutions need to evaluate and prioritize accordingly to help them achieve their desired goals while incorporating AI in surveillance. While the future prospect of AI in surveillance is exciting, it is imperative to understand that this is a long journey, and the optimal way to progress is through an effective collaboration between firms and regulatory authorities in taking this forward.

# Contacts


**Roy Ben-Hur**
Managing Director
Risk & Financial Advisory
Deloitte & Touche LLP
rbenhur@deloitte.com

**Adam Clarke**
Director
Risk Advisory
Deloitte UK
adamclarke@deloitte.co.uk

**Niv Bodor**
Senior Manager
Risk & Financial Advisory
Deloitte & Touche LLP
nbodor@deloitte.com

**Anand Ananthapadmanabhan**
Senior Manager
Risk & Financial Advisory
Deloitte & Touche Assurance & Enterprise
Risk Services India Private Limited
aananthapadmanabh@deloitte.com

**David Isherwood**
Senior Manager
Risk Advisory
Deloitte UK
davidisherwood@deloitte.co.uk

**Romit Deb Mookerjea**
Manager
Risk & Financial Advisory
Deloitte & Touche Assurance & Enterprise
Risk Services India Private Limited
rmookerjea@deloitte.com

**Nitin B S**
Senior Consultant
Risk & Financial Advisory
Deloitte & Touche Assurance & Enterprise
Risk Services India Private Limited
bnitin@deloitte.com

**Kewal Harshad Jagani**
Senior Consultant
Risk & Financial Advisory
Deloitte & Touche Assurance & Enterprise
Risk Services India Private Limited
kjagani@deloitte.com

**Subramanian Krishnan**
Senior Consultant
Risk & Financial Advisory
Deloitte & Touche Assurance & Enterprise
Risk Services India Private Limited
subrak@deloitte.com

**Anuj Khasgiwala**
Senior Consultant
Risk & Financial Advisory
Deloitte & Touche Assurance & Enterprise
Risk Services India Private Limited
akhasgiwala@deloitte.com

**S Goutham**
Consultant
Risk & Financial Advisory
Deloitte & Touche Assurance & Enterprise
Risk Services India Private Limited
sgoutham2@deloitte.com

# Endnotes


1. Financial Industry Regulatory Authority (FINRA), "Deep learning: The future of the Market Manipulation Surveillance Program," ***FINRA Unscripted*** podcast (ep. 98), January 25, 2022.
2. Deloitte, "How artificial intelligence is transforming the financial services industry," accessed April 2024.
3. FINRA, "Deep learning: The future of the Market Manipulation Surveillance Program"; FINRA, "AI applications in the securities industry," from ***Artificial intelligence (AI) in the securities industry***, June 2020.
4. FINRA, "Section II: Potential applications of quantum computing in the securities industry," from ***Quantum computing and the implications for the security industry***, October 2023.
5. Financial Conduct Authority (FCA), ***Market Watch 76***, January 2024.
6. Deloitte, "Deloitte launches new Generative AI-powered solution on RelativityOne and Relativity Server to help organizations accelerate document review, employee conduct investigations, PII identification and compliance activities," press release, January 22, 2024.
7. FINRA, "Key challenges and regulatory considerations," from ***Artificial intelligence (AI) in the securities industry***, June 2020.
8. Deloitte, "Trustworthy AI™," accessed April 2024.

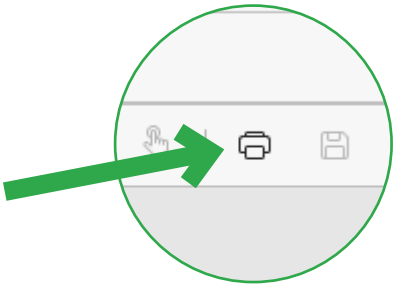
Deloitte.

# Printing instructions

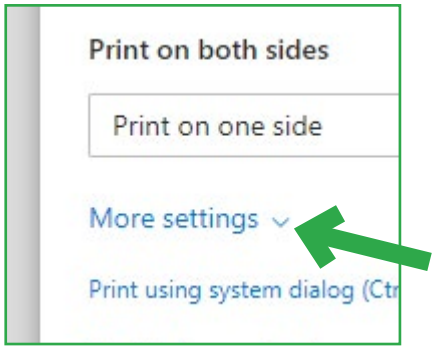
When printing through your web browser using the default settings, white bars may appear on the top and bottom of a letter-size sheet (8.5”x11”). To avoid this, either print on a legal-size sheet (8.5”x14”) or follow the instructions below:

**If printing through Microsoft Edge:**

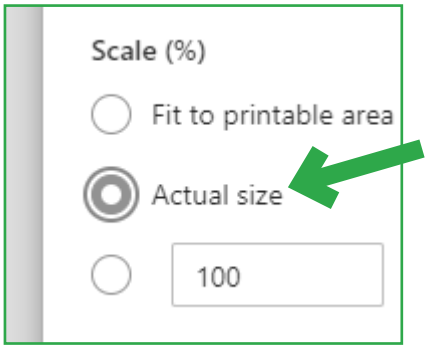
1. Click on the print icon.



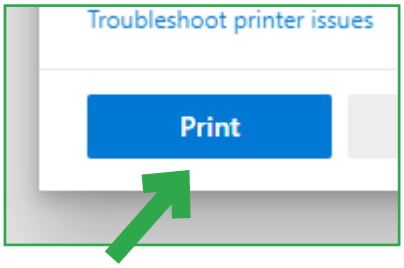
2. Scroll down to “More settings” and click to expand the menu.




3. Change “Scale (%)” to “Actual size.”

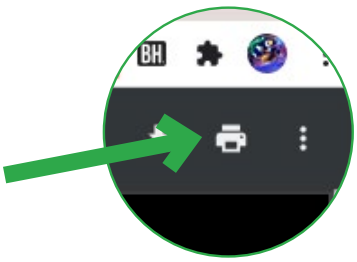



4. Click on the print button to print the document.

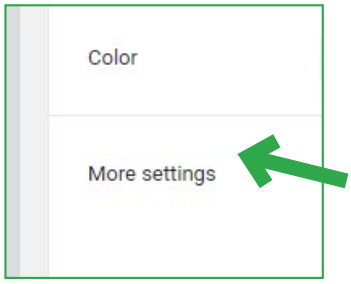



**If printing through Google Chrome:**

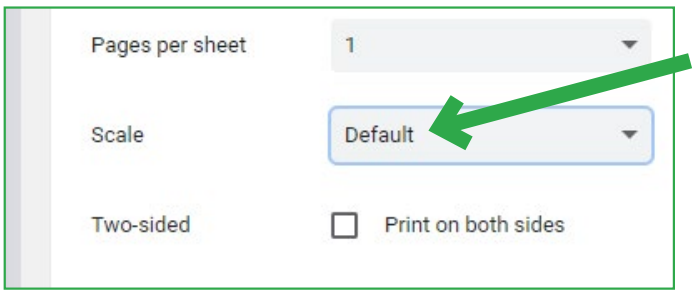
1. Click on the print icon.



2. Scroll down to “More settings” and click to expand the menu.




3. Change “Scale (%)” to “Default” (if needed).




4. Click on the print button to print the document.