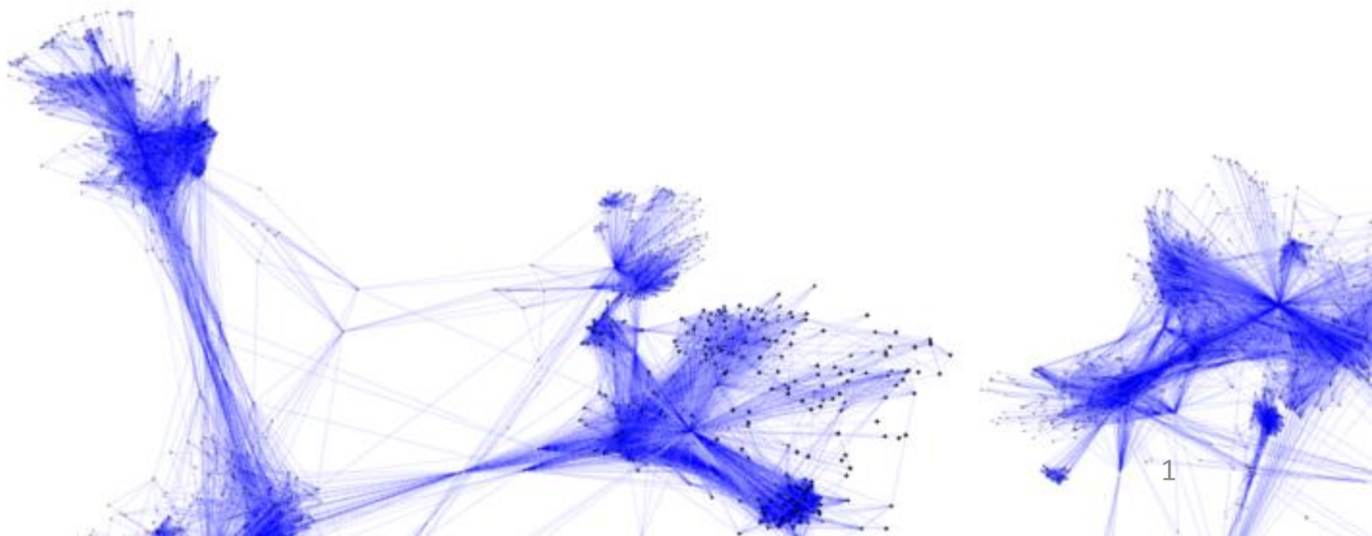
Summary of the report ‘Machine learning in UK financial services’ by BoE and FCA

October 2019

https://www.bankofengland.co.uk/-/media/boe/files/report/2019/machine-learning-in-uk-financial-services.pdf



Machine Learning in UK Financial Services (1)

- **Machine learning (ML) is increasingly being used in UK financial services**
- Survey over 106 financial firms, including banks, credit brokers, e-money institutions, financial market infrastructure firms, investment managers, insurers, non-bank lenders and principal trading firms
- **ML does not necessarily create new risks, but could be an amplifier of existing ones**.
- Such risks, for instance ML applications not working as planned, may occur if model validation and governance frameworks do not keep pace with technological developments.

→ https://www.bankofengland.co.uk/-/media/boe/files/report/2019/machine-learning-in-uk-financial-services.pdf

Machine Learning in UK Financial Services (2)

- The most **common safeguards with ML are alert systems and ‘human-in-the-loop’** mechanisms.
- **Firms validate ML applications before and after deployment**, mostly by outcome-focused monitoring and testing against benchmarks.
- Most users **apply their existing model risk management framework to ML applications**.
- But many highlight that these frameworks might have to evolve in line with increasing maturity, sophistication, scale and complexity of ML applications.

→ https://www.bankofengland.co.uk/-/media/boe/files/report/2019/machine-learning-in-uk-financial-services.pdf

Risk Management (1)

- Several firms highlight the need for their **risk management frameworks** to evolve given their increasing use of ML.
- Firms note that **explainability plays an important part in ML** model development, standards and governance procedures.
- The EBA Guidelines on Information and Communication Technology (ICT) Risk Assessment highlight that the ‘depth, detail and intensity of ICT assessment should be **proportionate to the size, structure and operational environment of the institution as well as the nature, scale and complexity of its activities**’

Risk Management (2)

- **ML models are often complex, very large, non-linear and non-parametric** making it harder to comprehensively understand their properties and how to validate them.
- **ML use can alter the nature, scale and complexity of IT applications** and thus, a firm's IT risks

Figure 1 Examples of risks and possible ways to address these

	Model validation	Staff and governance	Data quality
Example	'Black box' ML models are harder to explain and make decisions outside their original parameters	Staff may be insufficiently trained to understand and address risks related to ML models	Poor quality data, limited training data or biases may produce unintended and negative results
Possible ways to address the risk	Evolve model validation approaches — see section 5.4	Ensure employees have the right skill sets — see section 3.2	Apply data quality validation framework — see section 5.2 and 5.4
Safeguards	Alert systems, 'guardrails', human-in-the-loop before execution, kill switches and back-up systems — see section 5.5		

Risk Management (3)

- **The deployment of ML could also reduce risks** by reducing human bias, support the identification of market abuse practices, increase the effectiveness and efficiency of fraud detection and AML processes, as well as lead to better risk assessment and management
- **Model validation and governance need to keep pace with machine learning developments**.
- The survey responses suggest that ML applications can increase the technical complexity of models, and thus risk management and controls processes will need to keep pace.
- **Firms do not think the use of ML necessarily generates new risks. Rather, they consider it as a potential amplifier of existing risks.**

Risk Management (4)

- **Risks could be caused by a lack of ML model explainability.** This forms part of more general questions around validating the design and performance of ML models.
- **Models may perform poorly** under certain circumstances, like when being applied to a situation that they have not encountered before or where human experience, institutional knowledge and judgement is required.

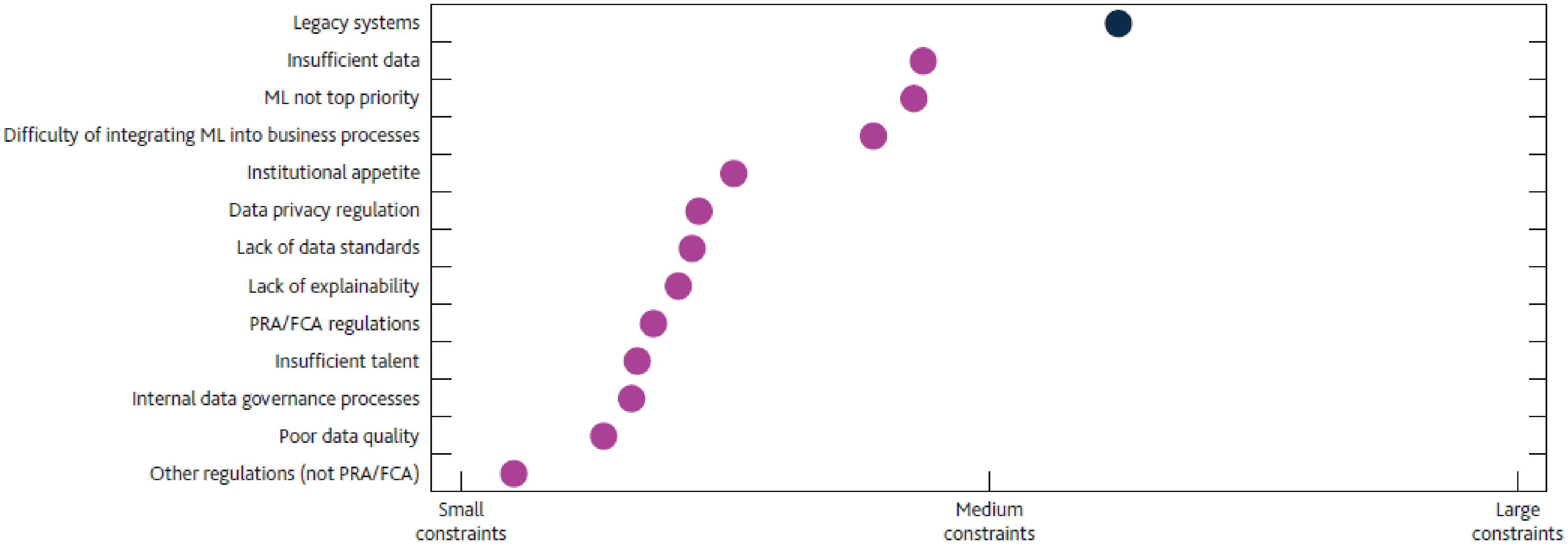
Risk Management (5)

- Respondents think the top five risks that might occur because of ML applications relate to:
    1. Lack of explainability
    2. Biases in data and algorithms
    3. Poor performance for clients/customers and associated reputational damage
    4. Inadequate controls, validation or governance
    5. Inaccurate predictions resulting in poor decisions
- We can summarise these into three overall categories: **model performance, staff and governance, and data quality with model performance being the most important.**

Constraints of Deployment (1)

- Several Constraints to the deployment of machine learning are mostly internal to firms.

Chart 11 Legacy systems are the largest constraint to machine learning deployment[(a)]



(a) Small constraint was allocated a score of 1, medium was 2 and large was 3.

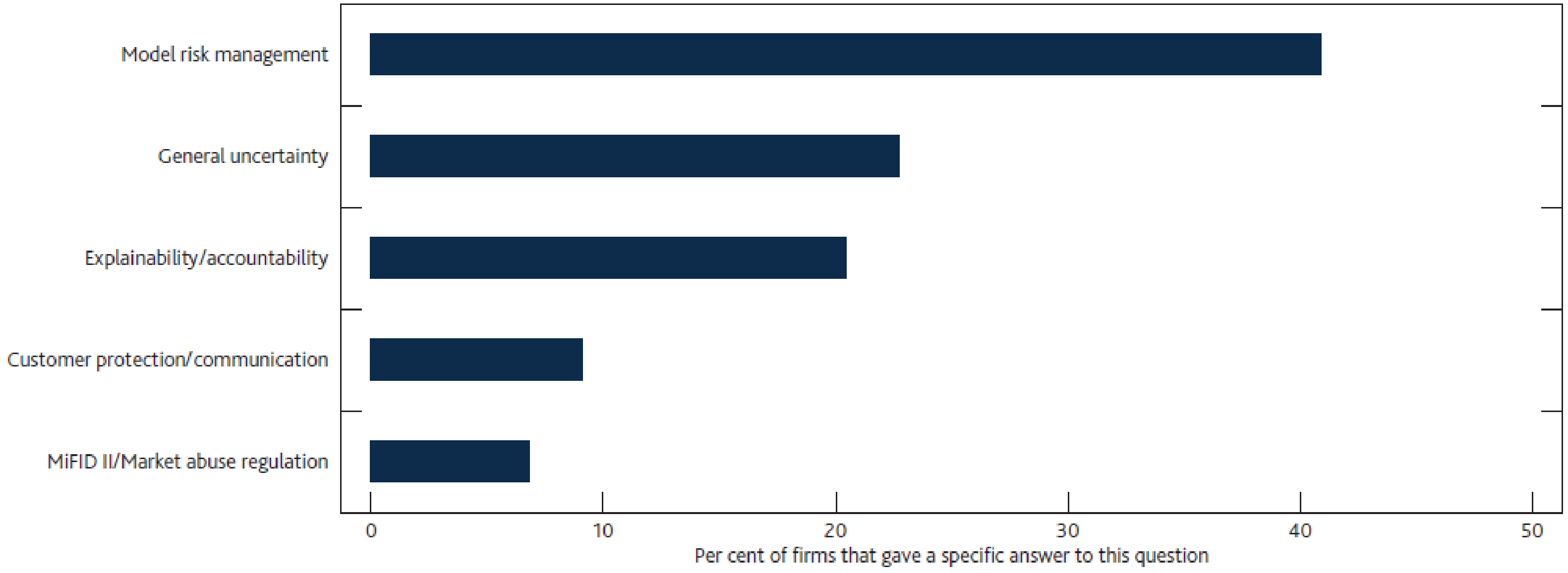
Constraint of Deployment (2)

Chart 12 Firms report constraints across a number of issues, but none are perceived as big

Challenges (1)

- **Challenges of meeting regulatory requirements to explain decision making** when using so-called 'black box' ML models are shown in Chart 13.
- A lack of clarity and uncertainty around how existing regulations apply to ML is observed. This could indicate that in the future regulation may need to be updated or adjusted.

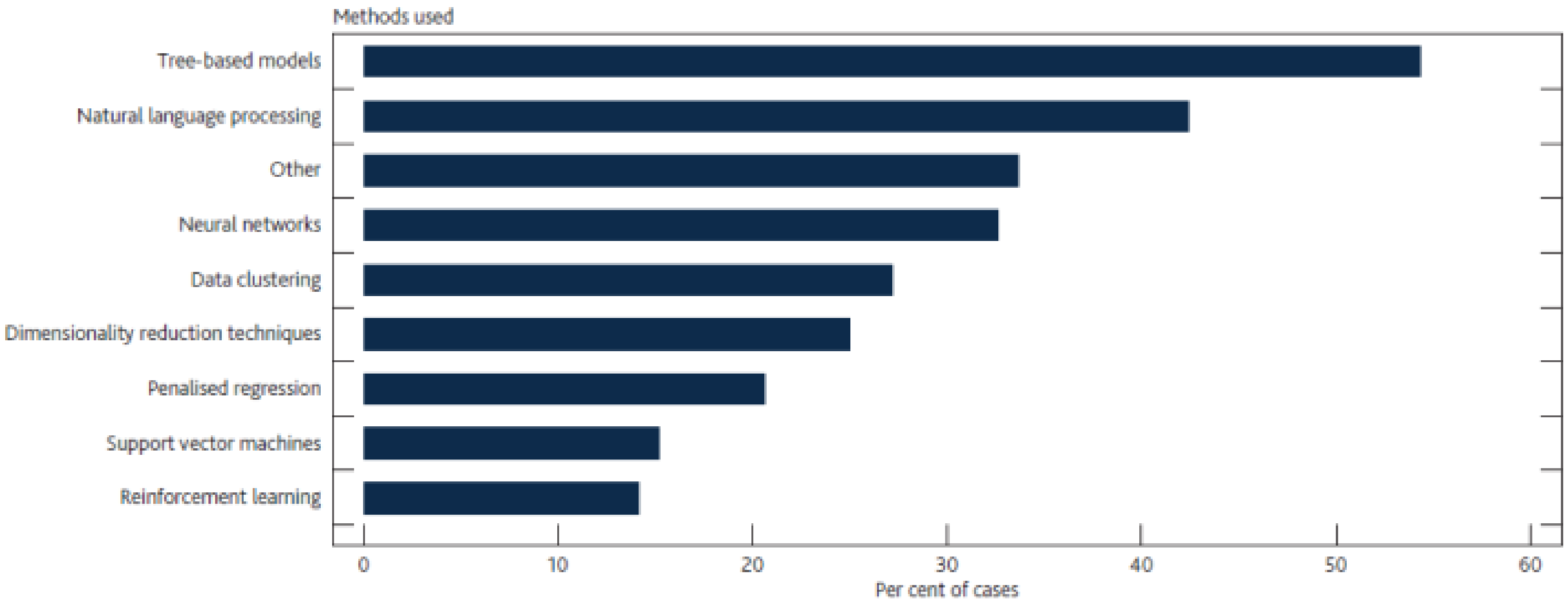
Chart 13 Firms identify model risk management as the one where regulatory constraints are most significant



Challenges (2)

- **Model engineering and performance evaluation decide which models are deployed:** the ML methods most often used are on the more complex end of the current spectrum.

Chart 15 Tree-based methods are the most popular techniques reported by firms[a][b]



(a) Firms often use more than one method at a time which is why the percentages add to more than 100.
(b) The underlying data is based on the use cases provided by survey respondents.

Challenges (3)

- **ML methods are more difficult to interpret than traditional linear regression models**, because they are ‘non-parametric’.
- Increased complexity makes model validation harder, which can translate into a potential risk.
- Validation methods can address this, but **new methods will likely be required, as ML techniques develop.**
- **Model validation is key to ensuring machine learning models work as intended:** Explainability techniques were used in less than half of the cases of the Bank of England study.

Validation Frameworks

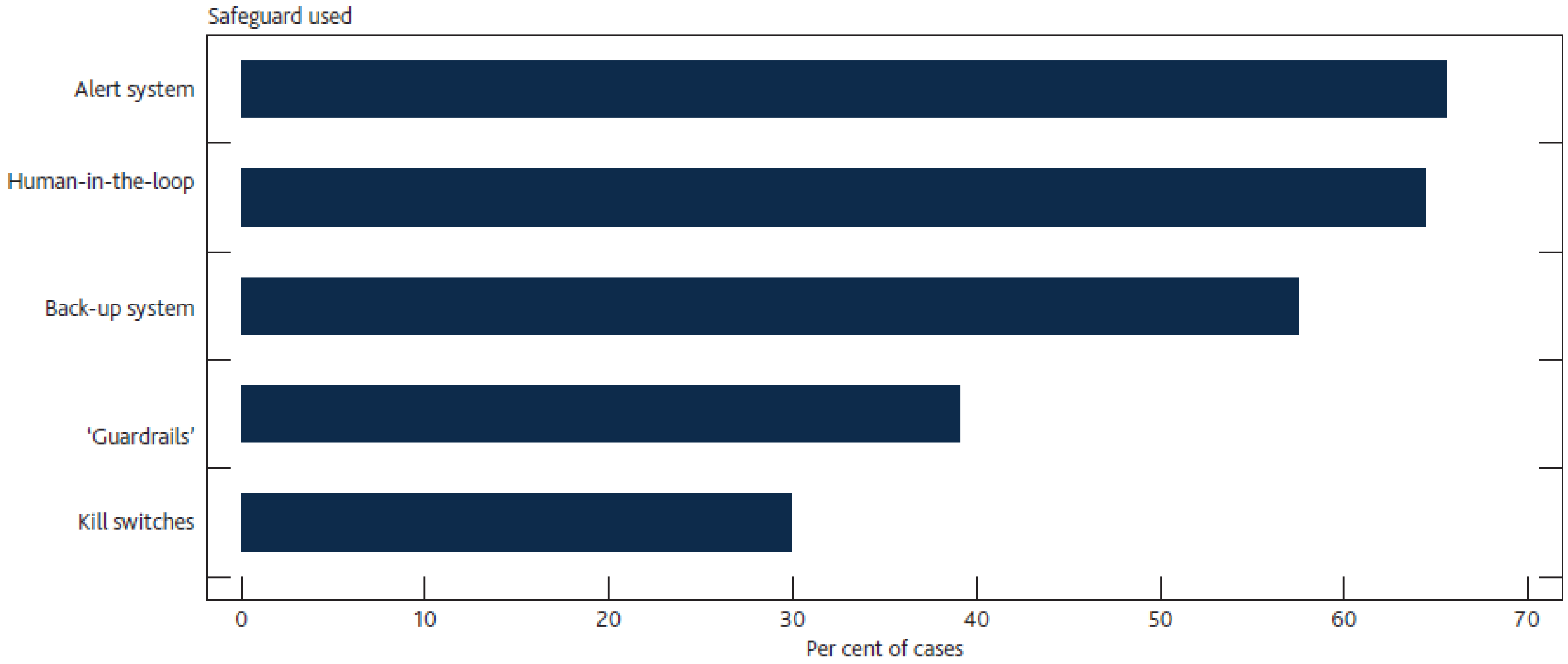
- **Many firms emphasise that validation frameworks still need to evolve** to address challenges associated with the nature, scale and complexity of ML applications. Therefore the use of some validation techniques may increase in the future.

Table 3 Firms use a variety of model validation techniques to assess machine learning model robustness

Validation method	Description
Outcome monitoring against a benchmark	Decisions or actions associated with the ML system are monitored using one or multiple metrics. Performance is assessed against a certain benchmark value of those metrics.
Outcome monitoring against non-ML model/ A-B testing	Decisions or actions associated with the ML system are monitored using one or multiple metrics. Performance is assessed by comparing it to the performance of a separate, non-ML model. The same approach is used in A-B testing (also known as split testing).
'Black box' testing	Input-output testing without reference to the internal structure of the ML application. The developer 'experiments' with the model, feeding it different data inputs to better understand how the model makes its predictions.
Explainability tools	Tools aimed at explaining the inner workings of the ML model (going beyond input-output testing).
Validation of engineered features	Engineered features used in the ML application are scrutinised, including potential impacts on model performance.
Data quality validation	One or more techniques are used to ensure potential issues with data (such as class imbalances, missing or erroneous data) are understood and considered in the model development and deployment process. Examples of these include data certification, source-to-source verification or data issues tracking.

Safeguards

- Firms use a range of safeguards to address risks: the **additional complexity, issues with explainability and the continuous lifecycle of ML introduce new challenges**, which require safeguards.

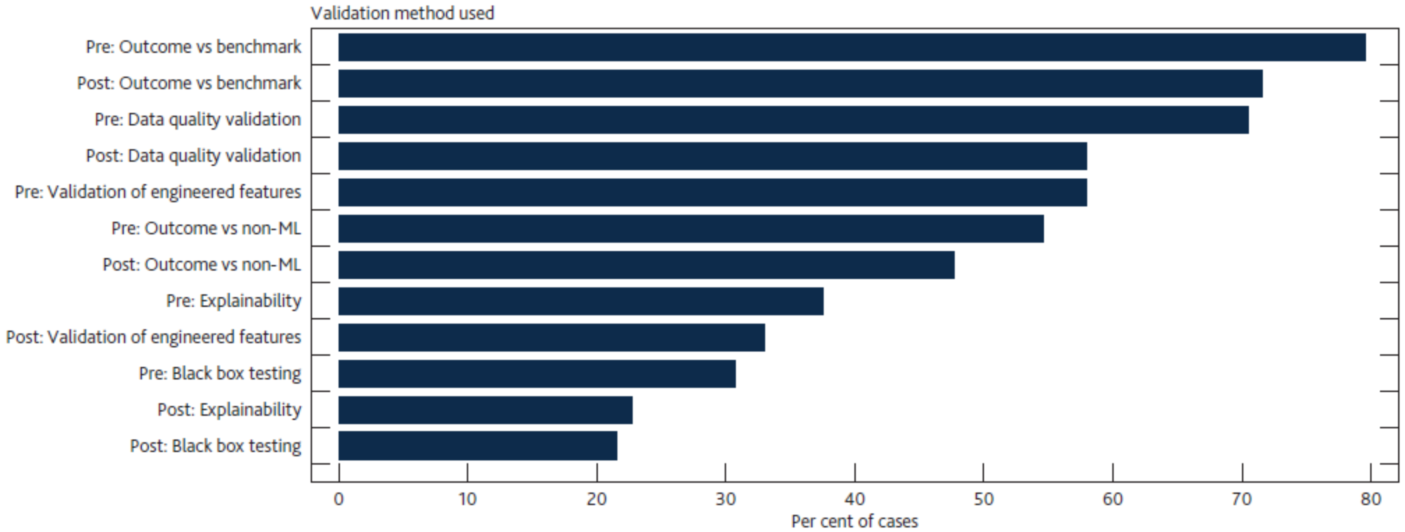


(a) Firms often use more than one type of safeguard at a time which is why the percentages add to more than 100.
(b) The underlying data is based on the use cases provided by survey respondents.

Conclusion

- **Firms report they are benefitting from the deployment of ML**
- Firms are keen to improve their validation frameworks for testing ML models work as intended. For instance, this includes approaches that help to make ML models more explainable.
- Where ML applications automate more of the decision-making process, explainability becomes more of a priority for firms.

Chart 16 Outcome-based validation methods are the most common[(a)(b)(c)]



(a) 'Pre' indicates pre-deployment use of the validation method. 'Post' indicates post-deployment use of the validation method.
(b) Firms often use more than one validation method at a time which is why the percentages add to more than 100.
(c) The underlying data is based on the use cases provided by survey respondents.

Software Partner for Applied Financial Data Science & AI

Dr. Jochen Papenbrock
jp@firamis.de

InvestTech | RiskTech | RegTech | SupTech