

## DECISION ANALYTICS

**Decision Analytics can be described as making sense of data in an effort to arrive at valuable decisions. The power of Decision Analytics is the creation of models that distil enormous amounts of complex and noisy data into scores, thus providing accurate insight into the risk of every potential decision.**

Models are especially powerful, driving real-time decisions in high-volume environments such as issuer screening of authorisations for fraud. Here, manual review of each transaction is impossible yet the requirement for real-time evaluation exists. In this example, models built using a blend of analytical techniques and artificial intelligence can provide a score helping the issuer make a real-time quantifiable decision on whether to accept the transaction.

Risk IDS are experts at risk-management models in the payments industry.

### How are Risk IDS Models different?

The Risk IDS modelling ethos is very different.

#### Intimate Business Understanding

Risk IDS believe that the best models come from those who understand the business intimately and can creatively construct relevant characteristics from data. A Risk IDS model is the product of a strict proven methodology that yields highly accurate, statistically relevant and above all, explainable models.

Risk IDS targets models only at markets where we have deep understanding of the business.

- **Issuing**  
Transaction Fraud Anomaly Detection and/or Classification  
Anti-Money Laundering Anomaly Detection and/or Classification
- **Acquiring**  
Merchant Anomaly Detection  
Anti-Money Laundering Anomaly Detection and/or Classification
- **Merchant**  
Merchant Transaction Fraud Anomaly Detection and/or Classification  
Anti-Money Laundering Anomaly Detection and/or Classification

#### Explainable Characteristics

Traditionally, models have been seen as a 'black box' where the end user has no insight into how a score has been created. The Risk IDS Approach to modelling provides a clear explanation of all characteristics that have contributed to a score.

#### Balanced use of Neural Networks and Statistical techniques

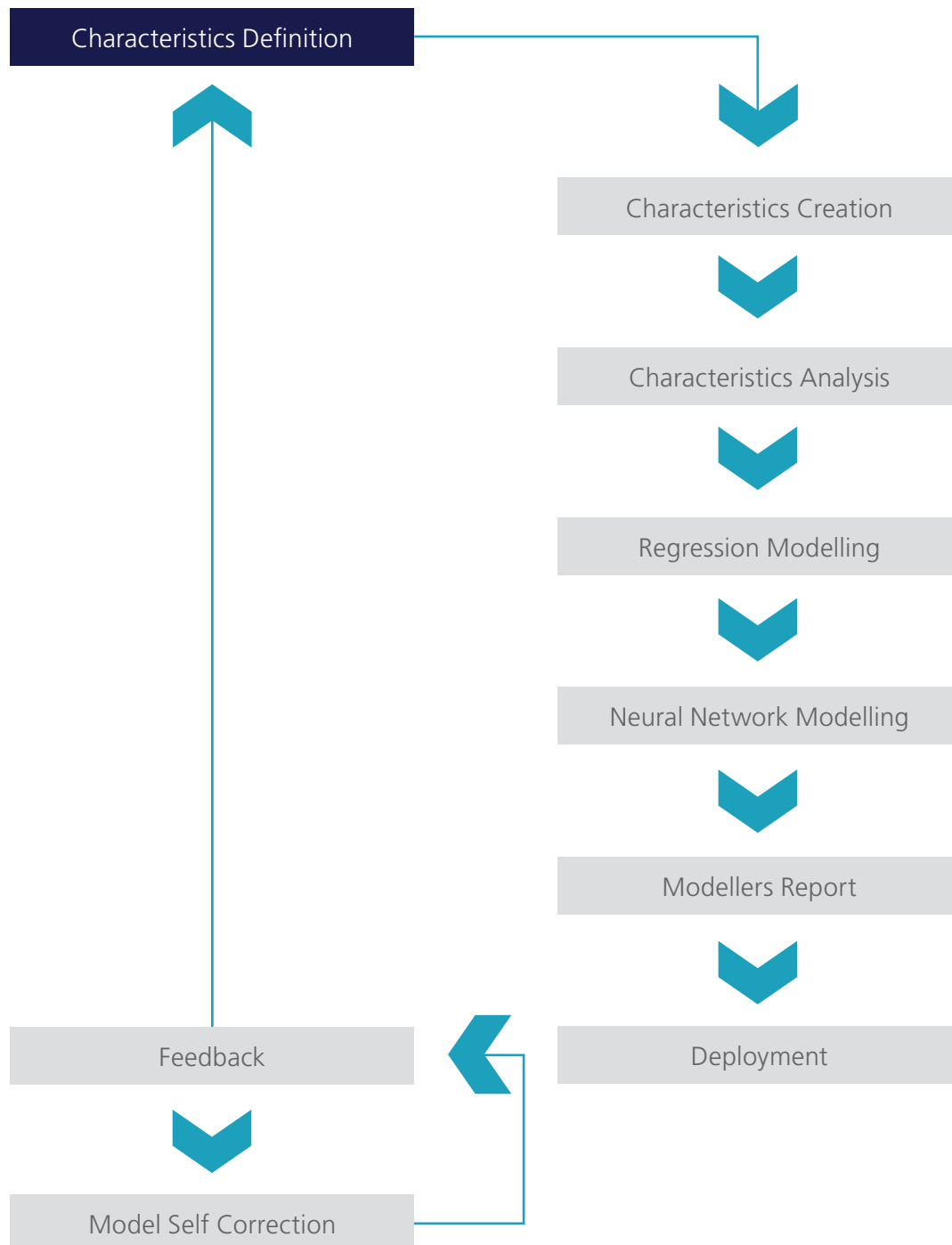
Risk IDS Models are balanced to utilise the power of artificial intelligence, which is inherently 'black box' with explainable techniques including ratios, binning, 80/20 principle (Pareto principle) and regression. The majority of the model remains highly explainable while the power of artificial intelligence is still harnessed.

#### Utilisation of Commercial Neural Network Technologies

Risk IDS uses commercial, off-the-shelf applications to create Neural Networks, which provides cutting-edge artificial intelligence techniques, without Risk IDS having to retain the deep artificial intelligence skills on staff. This approach allows us to focus on the business problem more closely thus making better models.

## Risk IDS Decision Analytics Methodology

Risk IDS Models are the product of a strict and proven methodology, which is described in the diagram below:



### Characteristics Definitions

Risk IDS will consult with the customer in what they believe are contributing characteristics, which will be in conjunction with the insight Risk IDS has, including known characteristics.

As an example for transaction fraud, a customer may believe that a transaction from France is problematic. Whether the characteristics defined are in fact valid or a judgemental bias at this stage is not important. This stage of the process could almost be defined as a brainstorming session and is intrinsic to the creative nature of the methodology.

### Characteristic Creation

Once the customer has defined the contributing characteristics — as they see them — Risk IDS creates these characteristics into a dataset ready to have a modelling process executed against it. At this stage, Risk IDS will make creative use of risk ratios, binning, 80/20 principle and other analytical techniques.

### Characteristics Analysis

At this point, it must be decided if any of the characteristics that have been created have validity. Typically, the characteristics modelled are littered with judgemental bias, availability bias being the more common (just because someone remembers an occurrence does not necessarily make it relevant). Risk IDS will now select what characteristics are useful for predicting risk and drop the rest. Although this seems wasteful — considering the characteristics have been conceived and constructed — it is intrinsic in obtaining highly creative yet valid characteristics.

### Regression Modelling

Using these characteristics, a regression model will be created, producing a score with strong statistical validity and highly explainable weightings.

### Neural Network Modelling

Just because a characteristic failed correlation or did not quite make it to the regression model does not always mean they are completely discarded. A Neural Network, classification or anomaly detection, is brought to bear to provide a final score on the broader more noisy set of characteristics including the regression score. From the end user's perspective, the outcome of the neural network is highly unexplainable but tends to be extremely accurate.

### Modellers Report

The culmination of the modelling process is the Modellers Report, which describes the contributing characteristics and whether this is used in the regression score prior to the Neural Network. Crucially, the modellers report describes the effectiveness of the score at a variety of thresholds.

### Deployment

Risk IDS Models integrate seamlessly into the Risk IDS...zero cost. A score is enriched into a record being processed in the Decision Engine allowing the score, perhaps blended with further rules, to influence a decision real-time.

### Feedback & Adaptation Loop

Neural Networks are adaptive systems, which are able to adapt their behaviour according to changes in their environment or in parts of the system itself. This would also be described as self-correction or self-learning. Risk IDS models, optionally, can be deployed to self-learn based on feedback data.

However, practically self-learning is achievable only up to a certain point before a model rebuild is required. Self-learning in certain scenarios is often not suitable at all. Typically, a rebuild is required around every twelve months depending on the risk problem.

---

### Next Step

For more information about how Risk IDS Decision Analytics can be integrated into your payments business, email [contact@riskids.com](mailto:contact@riskids.com) or call +44 (0)20-3287-0213