UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M. FANNO"

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

"Analysis of operations against organised crime conducted by EUROJUST"

RELATORE:

CH.MO/A PROF./SSA Parbonetti Antonio

LAUREANDO/A: Manzi Andrea

MATRICOLA N. 2031879

ANNO ACCADEMICO 2023. – 2024

Dichiaro di aver preso visione del "Regolamento antiplagio" approvato dal Consiglio del Dipartimento di Scienze Economiche e Aziendali e, consapevole delle conseguenze derivanti da dichiarazioni mendaci, dichiaro che il presente lavoro non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere. Dichiaro inoltre che tutte le fonti utilizzate per la realizzazione del presente lavoro, inclusi i materiali digitali, sono state correttamente citate nel corpo del testo e nella sezione 'Riferimenti bibliografici'.

I hereby declare that I have read and understood the "Anti-plagiarism rules and regulations" approved by the Council of the Department of Economics and Management and I am aware of the consequences of making false statements. I declare that this piece of work has not been previously submitted – either fully or partially – for fulfilling the requirements of an academic degree, whether in Italy or abroad. Furthermore, I declare that the references used for this work – including the digital materials – have been appropriately cited and acknowledged in the text and in the section 'References'.

Firma (signature) …….……

Abstract

Purpose and Scope

Our goal is to find red flags in detecting financial crimes, through a risk management models, based on the operations against organized crime conducted by Eurojust.

Methods or Approach

We used a top-down method.

1. collected a dataset of financial crimes, from the beginning of 2017 to 2024
2. categorized the financial crimes within 4 categories on which Eurojust conducted operations: I) Fraud and swindling; II) Money laundering; III) Corruption; IV) PIF
3. collected and analyzed single case studies of well-documented financial crimes, based on which we obtain the main red flags of fraudulent activity.
4. we finally built a model to quantify the level of risk of fraud to each scenario testing it and obtaining the result.

Results

Results positively showed the findings of pattern useful to identify fraud risk, and specific variables on which the models used to forecast risk have to focus, such as transaction; assets; source of financial statements elements; regulations fulfillment.

Acknowledgement:

Thanks to **all the professors** for their teaching over the years, to all **those who provided me with information and advice** for the objective of the thesis, and specifically, a special thanks goes **to my supervisor** *prof Antonio Parbonetti*, who guided me through all the thesis work and made all this possible.

Also, a special thanks to:

- *Davide Moles* and *Paolo Manetta* from *Re-Lender S.P.A*. who gave me highly valuable information to focus on for this thesis.
- *Saajan Sharma Nepal* who jointly with *Andrea Ferrero* from *Young Platform* gave me insights about AML and financial crime red flags in Crypto industry
- *Dan McCrum* from *Financial Times,* who spent years to research about Wirecard fraud case, and endured threats and intimidation and who gave me good guidance about red flag identification.
- *Ton van Lierop*, Spokesman of Eurojust, for his useful responses, and the *Legal Affairs Unit.*

A last and very felt endorsement goes to *Ms. Daphne Caruana Galizia* who bravely exposed the ABLV Bank fraud and paid with her life the price of exposing criminality and corruption.

It's also for her and other many people who endured threats or paid the ultimate price, that we must act rightfully in detecting and condemning financial crimes.

Index

1. Introduction

Eurojust commitment to contrast organized crime is well established facing lot of challenges in coordinating multiple member state regulations. This difficulty was also one of the motivations for OCGs to increment activities in various member states, simultaneously, using for their advantage the different regulations in different countries.

I must admit that the all-thesis procedure aimed to find a unique solution for modeling risk of incurring in a financial crime, wasn't easy, and this thesis itself is not a final solution but a starting point for more advanced developments.

Thesis goals included: I) understanding how much financial crimes weighted on Eurojust total crimes investigation, and how those financial crimes could be prevented; II) Detect red flags that signal the presence of a financial crime, by developing a standardized model.

The top-down approach used to obtain the result, was the perfect strategy because we started from more than 85.000 cases in the last 7 years, 73% of which were financial crimes, or fraud related crimes, to a few hundred of case studies sample, which weren't easily collectable seen the nature of the investigation about them.

Finally, starting from the binary classification of risk, to show if the indicated variable was present (equal to 0) or not (equal to 1) we were able to obtain a decision tree scenario with around *1.073.741.824* scenarios, each with different risk dimensions.

Value of variables and sub-variables were calculated considering a multitude of categories of cases, mainly through z-score method, impact score ranking (1-7), and geometric mean.

We used this modeling strategy to fairly evaluate risk value through ex-post, based on every specific case of application.

The results leave open to further research opportunities, such as the back testing through counter-proof cases, understanding if the model can be transformed into a standardized ex-ante risk valuation, which is why I chose to publicly make this thesis available.

2. Methodology

2.1. Dataset from Eurojust: 85.538 operations

We obtained a dataset from Eurojust operations, through press releases where Eurojust specifically disclose all the info about the case (2024, 2021)[1], and then raising more then 85k cases based on the annual reports.

During this dataset collection, we had certain goals in mind especially the one-off understanding how much financial crimes weighted on EU total crimes investigation, and how those financial crimes could be prevented.

To understand how to prevent any type of case, it's fundamental to leverage the useful work made by Eurojust in these years, and divide the crimes per category, and by that generating a testing sample of companies involved in those crimes.

Classifications is made:

- Classification through crime types: based on their annual reports, from 2017 to 2023

CRIME TYPES	2017	2018	2019	2020	2021	2022	2023	*Total*
Financial crimes	2.812	3.324	3.915	3.809	4.413	5.084	5.835	*29.192*
swindling and frauds	1.630	1.924	2.262	2.654	3.135	3.687	4.190	*19.482*
money laundering	858	1.041	1.265	1.472	1.672	1.887	2.224	*10.419*
corruption	197	222	250	287	327	311	354	*1.948*
PIF crimes	127	137	138	217	251	263	292	*1.425*
Drugs	719	896	1.003	1.169	1.602	2.116	2.462	*9.967*
Human traffiking	287	343	399	390	342	329	326	*2.416*
Cycbercrimes	176	218	247	334	398	442	534	*2.349*
Migrants smugglings	153	157	187	224	303	336	425	*1.785*
Mobile organised crimes	482	541	598	381	800	862	1.000	*4.664*
Terrorism	177	190	222	217	220	202	205	*1.433*
Core international crimes	0	12	0	12	16	35	45	*120*
Environmental crimes	19	38	41	23	24	19	23	*187*
Intellectual property crime	0	0	0	27	31	39	54	*151*
Total	7.637	9.043	10.527	11.216	13.534	15.612	17.969	*85.538*

Table 2.1: crime time classification – EuroJust annual reports from 2023 to 2017

Based on this classification from 2023 to 2017[1], we understood that not only financial crimes were the most frequent type, carrying an **average weight over the year of 56.4%.** and the ones with most stable growth, with an annualized **CAGR of 11%.**

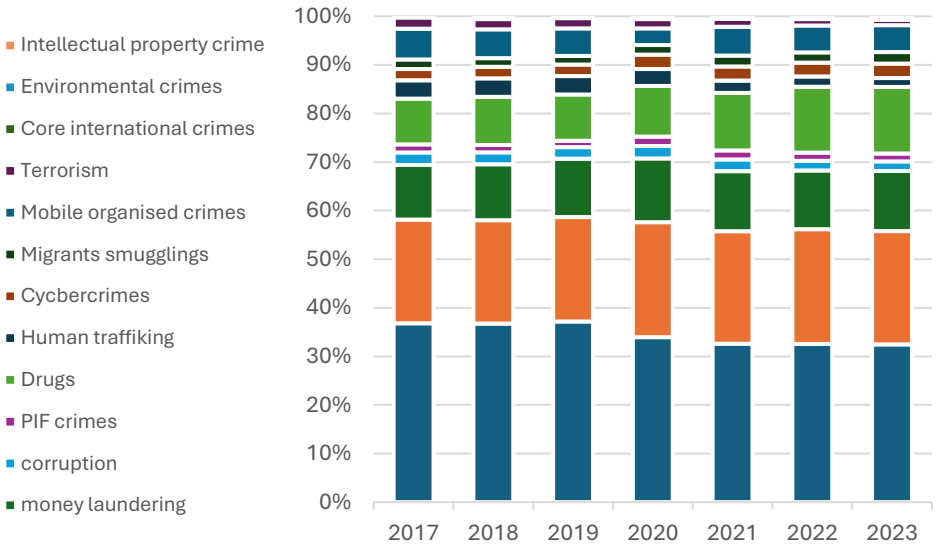

Figure 2.1: crime as % of total – EuroJust annual reports from 2023 to 2017

- Classification though countries involved: country that saw the biggest increase in this 5 years, are Latvia (217%), Luxembourg (171%), Portugal (154%), Bulgaria (144%), Sweden (133%) while the ones that saw more stability and lowest growth in new cases involvement are Germany (45%), Romania (44%), Poland (37%), Slovakia (32%), Denmark (9%).

- Classification through operations outcome:

Eurojust reported on the annual report starting from 2019, operations result from ongoing and open cases in the reference year. Damages refers to monetary compensation awarded to a party for loss or injury caused by another's wrongful act or breach of duty, and in this 5 years' period it summed up to 66B of dollars, which based on previous estimates about crime types, **13.5B are attributed to financial crimes**.

Info	from 2019 to 2023
Cases involving organized crime groups (OCGs)	7.601
Suspects	275.293
Arrests	14.343
Worth of damages (Mln)	66.156
Asset seized (Mln)	9.600

Table 2.2: operations outcome from Annual report by Eurjoust (2019-2023)

2.2. Case studies: 37 companies

The second step of the top-down analysis is, based on the categories identified as main priority in Eurojust operations, build a well-documented sample of companies sanctioned of a financial crime.

Companies have been identified based on: European Agencies investigation involvements (have been investigated in Europe, also by Eurojust); dimension and relevance of the case (monetary or reputational impact of the scandal/case), dimension and relevance of the company (known/big company), involvement into the type of financial crime on which Eurojust focuses on.

The goal during this phase was to **find the red flags** in each case and each category of crime.

How did we do it? Simply, based on financial statements of those companies as well as investigation reports or testimonial by contributors, all the info collected made possible the findings of patterns identified in frequent red flag per each case analyzed.

2.2.1. Categorization of information

Our first step was to associate cases by categories: **Fraud, Corruption, Money laundering**.

- **Fraud**, which following the ISA 240 (*2004, p.5, par.6*) definition is an intentional act by one or more individuals among management[2], can be of many types, but our focus was on *corporate fraud*, which is fraud committed by companies. In this category, we included *PIF*, which are crimes against financial interest of European Union[3], and *swindling* which is a fraud built through unfaithfulness or abuse of confidence[4].
- **Corruption** included bribing activity to politics and power authorities, to ensure contracts, reduce regulatory pressure or enable otherwise illegal activities.
- **Money Laundering** is the set of processes where illicit profits are transacted through legal activities to generate new cash out of the company. These transactions are made using shell companies, companies used as "shell", meaning non-active companies with near zero transaction, used only as legal entities for cover-up transactions.

Within the sample we compared the cases through 2-levels categories comparisons: fundamental and non-fundamental to model building.

- Non fundamental categories are: Crypto; Country; OGC, Source, Accomplices.

Crypto classified by 1 if the case involved crypto assets, cryptocurrencies or decentralized blockchain technologies and 0 if not.

Same thing for OGC, if the case involved or not Organized Group of Crime.

While country, source and accomplices are just specific information about those cases related to country of company involved (country), journalistic sources of investigation (source) and accomplices fined or clearly involved in the case (accomplices).

- Fundamental categories are: Estimated impact (Mln); Impact; Flag categories; Sub-flag categories.
    - Estimated impact in Mln of USD, is the total financial damage of the specific case on the company, either with fines or sanctions, but also in terms of total equity or market loss. In this context, choices of the right measure, depends on the case, following this model:

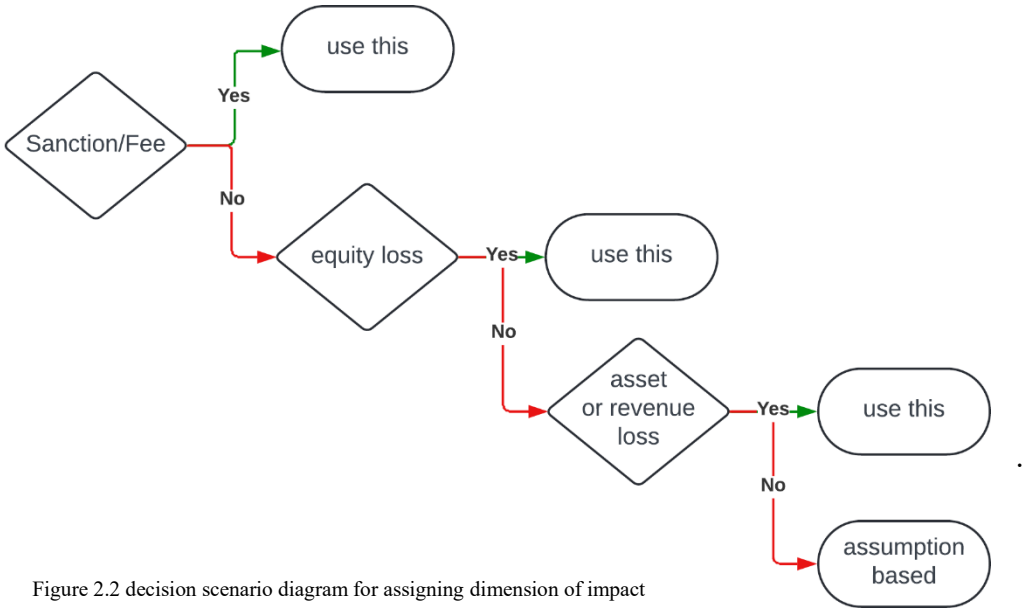

Figure 2.2 decision scenario diagram for assigning dimension of impact

When a company is directly sanctioned, damage is easy to quantify, however there are cases where there is no monetary sanction but only indirect damages, which impact financially the company through equity loss, asset freezing, revenue loss, or if not precise amount is given, we just assume based on given parameters.

- Impact parameter is a measure of damage, which includes also financial damages, but in relation to other measure of impact, and its levels classification is made by the analyst, in this case by me, assigning each case into the level that fits the most.

  The measure can assume values from the interval {1;7}:

    - **Level 7 - Catastrophic Impact**: Company closure or bankruptcy. Key executives and managers arrested or imprisoned. Significant financial losses for stakeholders.

        - **Level 6 - Severe Impact**: Major reputational damage. Substantial financial losses. Legal proceedings and fines.
        - **Level 5 - Significant Impact:** Reputational harm affecting customer trust. Financial losses impacting operations. Regulatory investigations and penalties.
        - **Level 4 - Moderate Impact:** Reputational damage but not critical. Financial losses manageable. Regulatory inquiries.
        - **Level 3 - Mild Impact:** Limited reputational harm. Minor financial losses. Internal investigations.
        - **Level 2 - Negligible Impact:** Minimal reputational damage. Negligible financial losses. Routine compliance checks.
        - **Level 1 - No Impact:** No noticeable consequences. Minor fines or inquiries.
    - Flag categories are the main aim of this model:

1. (**variables**): the red flag identified during the investigation, which will then be transformed into variables, when applying the model.
2. (**sub-variables**): variables (flag categories) have also sub variables (sub-flag categories), which are part of the variable matrix, which if present, creates a proportional change in value of the variable.
3. (**sub-categories**): sub variables have themselves another layer of specialization called sub-categories, part of the sub variable matrix, which if present, creates a proportional change in value of the sub-variable

$$\begin{bmatrix} a \rightarrow \begin{bmatrix} l \rightarrow [lag] \\ mo \rightarrow \begin{bmatrix} brf \\ cfc \\ mfc \\ bfd* \\ eot* \\ emi \end{bmatrix} \end{bmatrix} \\ t \rightarrow \begin{bmatrix} it \rightarrow \begin{bmatrix} tts^* \\ itu^* \end{bmatrix} \\ ot \rightarrow \begin{bmatrix} tsc \\ tfs* \\ hpi \\ thl \end{bmatrix} \\ ar \rightarrow \begin{bmatrix} lau \\ aic \end{bmatrix} \\ fm \rightarrow \begin{bmatrix} nfd \\ ntf \end{bmatrix} \end{bmatrix} \\ s \rightarrow \begin{bmatrix} em \rightarrow \begin{bmatrix} nsi \\ hce \\ hds \end{bmatrix} \\ rm \rightarrow [vma] \end{bmatrix} \\ r \rightarrow [fi \rightarrow [amy]] \end{bmatrix}$$

**sub-categories are identified as relevant to the model, but not found within the sample.*

Explanation of the variables:

- Assets (variable) includes all asset related flags of financial crime ($impact\ ratio$: $0{,}1396812\sigma$).

  Within this variable we found strong evidence of increase in risk related to:
  - location of assets owned by the company or with which the company transacted with (l)
  - however, to classify this risk using a fair valuation we used the Basel AML index 2023:
    - location of assets general risk, is a sub-category in which, assets located in countries with an overall score between: 8,25: Haiti – Max risk (100^{th} – 90^{th} percentile) and 6,05: Macao Sar China – High risk (90^{th} – 75^{th} percentile)
  - management & ownership, if the risk-flag is within the ownership board of the company, board of directors, or just within the assets held by the company (mo).
    - board figure/shareholders with clear interest in location with high risk, *(brf)* is a strong risk signal, typically in corruption and fraud cases.
    - CFO churn, or no management churn over long period, *(cfc)* which has been empirically tested positively for companies during their last phases of operation or anyway near the phase where fraud became almost clear.

        - Management misreported or misguided covering fraudulent schemes, *(mfc)* is a formal way of management lies on everything (as suggested my Mr. McCrum of FT)
        - board figure with shady details or not clearly disclosed *(bfd)*
        - effective ownership of activities not clearly traceable, *(eot)* as suggested by Davide Moles, is clearly a sign of lack of ownership of business operations, but during the model I integrated this sub-category into *(bfd)*
        - employees/managers/owner with multiple roles/duties/interest *(emi)* in company network of subsidiaries
- Transactions (variable) is the variable with the highest impact on total risk ($impact\ ratio$: $0{,}3472792\sigma$) and includes all transactions, both inbound and outbound, with certain evidence of risk in:
    - Inbound transactions, meaning all transaction directed towards the company. This sub-variable wasn't easy to detect during our research, but we found evidences of many cases where the financial crime could be linked through the clients transactions ($it-\ contribution\ to\ risk$: $0{,}712644291\sigma$) leading to a rise in risk. However, thanks to our external contributor, Davide Moles chief of compliance in Re-Lender S.P.A (complete interview further in the chapter), risk can increase if the inbound transactions to IGA countries comes from Israel or African countries, which are linked to weapons imports to countries where conflicts are still on. We found evidence also of many cases where risk was increased by transactions to employee for undisclosed works, typically considered an inbound transaction because happens between the managed account of the sales department and the employee with role of account management, however this was then revalued and integrated to the category of transactions to/through shell companies, within outbound sub-variable.
    - Outbound transactions are a key indicator to investigate on (ot). Typically, when investigating on corruption risk, this is the key sub-variable of the transaction variable matrix, especially when:
        - Outbound transaction directed to lag positive locations (*thl*). In this context, following the Davide Moles indication, there's a special accent of risk when transactions from IGA countries are outbounded to Balkans, (IGA countries are the weapons producers, typically).
        - Outbound transaction to/through shell companies (*tsc*) are a leading risk indicator. Within this sub-category we consider all transactions which company

directed to or through shell companies which typically are organized as a network;

- Within this context, highly political involvement within business interests (*hpi*), is a relevant key sub-category, which has been inserted into the outbound transaction because when the links connect multiple businesses to relevant politics, either through shared interests companies (as companies owned by politics and the business itself) either through political interest in the region or industry of relevant political interests. This sub-category is the most frequent within corruption category;

- Acquisition and restructuring *(ar)* sub-variable cover the operations of m&a which have been conducted through a type of loan () and those operations where there's no clear sign of profit out of the acquisition for highly indebted business. This sub-category, as we'll explain further in this thesis, has been a main signal of investigation both for FTX exchange both for Wirecard;
- Fund Misappropriation is a specific sub-variable that refers to fraudulent usage of equity capital or liquidity coming from financing flows. When there's no clear fund usage disclosure *(nfd)* or when no tax are paid or applied on those funds *(ntf);*

- Source of financial statements (variable) () includes all those elements such revenue, assets, expenses, liabilities which increase risk of financial crime $impact\ ratio$: $0{,}0503381\sigma$.
  - Revenue and Assets misreports (*rm*) includes all cases where the companies manipulate fraudulently revenue sources and fake pumping of it, assets valuation within balance sheet. Specifically, evidence have been found to notice relevant significance of risk increase when valuation of assets and revenue are manipulated (*vma*).
  - Expenses and Liabilities misreports (*em*) includes all the cases where the company fraudulently fake liabilities value or expenses attribution. Evidence have been found in company that shows high debt to suppliers or receivables (*hds*), no clear or shady suppliers' identification (*nsi*) and high share of expenses attributed to commissions/consultancy expenses (*hce*).
- Regulation fulfillment (variable) includes all the cases where the company is sanctioned ($impact\ ratio$: $0{,}0732768\sigma$) whether to a lack of AML procedures or a general failure in internal control systems (ICS). Typically, when companies receive multiple sanctions over the years *(amy)* there's significant risk that failure are not result of accident but fraud.

Variables identification process and contributions:

I had the privilege of having valuable contribution by professionals within the compliance and investigation sector.

Contribution, as showed in the variables, sub-variables and sub-categories explanations, were integrated in the research phase, before building the model, and many of the suggested thesis were effectively tested and proven with the model.

Davide Moles – Red flags in identifying financial crimes, literature and experience.

Chief of compliance of Re-Lender S.P.A, previously in Deutsche Bank, Ag Generali, Arbitro Bancario Finanziario and Unicredit.

His experience was useful for the better understanding of financial crime early signs.

- "Research shows that high entity dimension entities, correlates to higher risk of AML failure" ironically "because they're more exposed to being better choices for OCGs." This choice is made because OCGs needs to use high liquidity banks, to cash in and out illicit profit, and because if the choice would be a small bank, transaction detection risks grow.
- Transactions leads the way in early signs detection, especially if to or through non-productive assets (no transactions) better known as shell companies. But once more the current macro context tells us that location of the transaction parties, are fundamental to detection processes. In fact, transactions referencing Italy, Germany, Austria (IGA) outbound to Turkie or Balkans countries and Italy, Germany, Austria (IGA) inbound from Israel, Palestine or generally African countries with active conflicts), requires many attentions during AML procedures.
- Board figure with no clear referencing or identification, as well as no clear effective ownership owner identifiable are also good risk indicators.
- In conclusion transaction or ownership by sovereign states funds such UAE, Russia, Qatar and so on, typically monarchies that don't fully co-operates with UN convections, such BRICS countries, could be a sign of risk, because typically in those countries, states fund have low levels of bureaucracy and typically incur less scrutiny compared to highly regulated US or EU countries. However, I couldn't quantify this flag in my research, as there are no, in my opinion, relevant indicators that objectively classify this kind of risk, such the Basel AML Index[4] for AML failures.

Saajan Sharma Nepal, AFC of Young Platform

AFC Specialist of Young Platform, a FinTech startup managing first Italian crypto exchange, gave me strong insights on risks about transactions and red flag identification, specifically within crypto-assets industry.

- "Given the inherent risk of each transaction, when talking about virtual currencies they're relatively traceable" and added "we have strong accuracy in detection of destination, however not about the recipient" which as he says "that's what, those who goes against digital currencies, typically uses as main claim against this type of product"
- "I agree with you about transaction being main red flag, in detecting financial crime risks" as he said, typically technologies, also used by Young Platform, uses abnormal pattern recognition, which returns suspect feedback.
- In companies that operates as exchanges, as YoungPlatform, control starts from onboarding until account closure, from location to means, such as network used, frequency of transactions, type of deposit.
- In the context of YoungPlatform, the software is very advanced and the datapoints and variables are I) transaction, II) subject profile, III) location of the asset and subject, IV) age group. Age group is a standardized categorization strategy to create risk profiles, considering younger customers less risk-adverse while older customers, more risk adverse and shorter time-horizon.

Dan McCrum from Financial Times

Mr. McCrum works as journalist for Financial Times since 2007, and I asked for his contribution regarding Wirecard scandal, which he discovered.

- "Management lying about anything" especially within Wirecard, FTX, 1MDB, RBS GRG has been overly proved, and the quantification of this investigation hint was categorized within: *management misreported or misguided covering fraudulent schemes (mfc), board figure with shady details or not clearly disclosed (bfd)* and also in line with Davide Moles information about *effective ownership of activities not clearly traceable (eot*)*
- "Receivables" or also short-term debt towards suppliers, included within current liabilities, which are debts to be extinguished within 12 months, "growing faster than sales". Here the info was empirically proven and integrated within *high debt to suppliers (hds)*

- "CFO churn" which is the change of persons in charge of CFO position, typically happening, as explained before and "no management churn over long period" which implies that over time, board of managers never change.
- "Trend of rising debt at a cash flow positive company" is obviously a sign of "fake" cash representation, which are not clearly representing the overall health of the company.

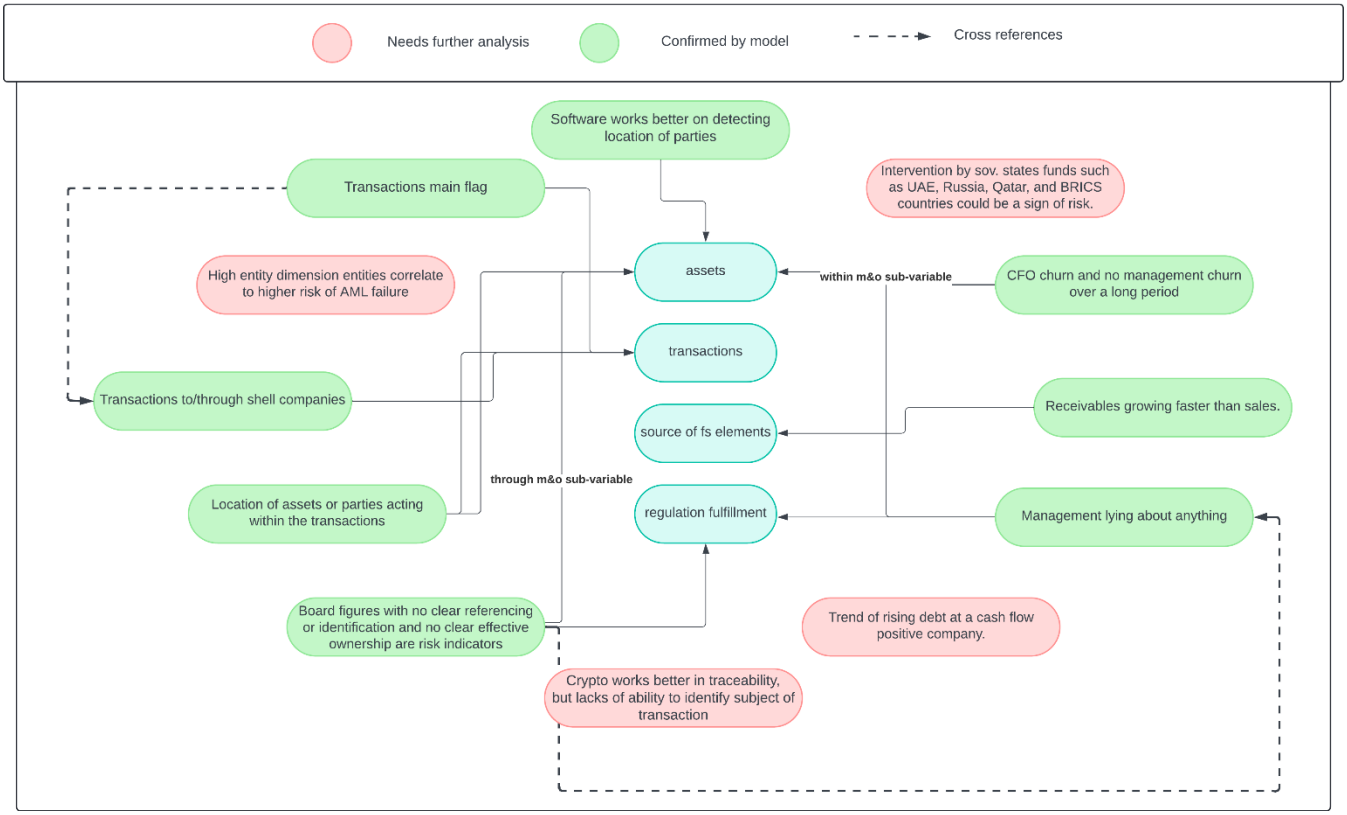

Figure 2.3: cross-references networks of contribution – categorization within variables and further analysis needs, judgment,

2.3. Model

Our goal was to create a model to assign risk value appliable through our ex-post sample analysis that assign a y value to each company, based on the flags showed, in a standardized manner.

We wanted to assign a value to these variables, so the first step was to cross a decision tree, with binary choices (0 = not present, 1 = present):

$$\begin{Bmatrix} 0 = flag\ is\ not\ shown \\ 1 = flag\ is\ shown \end{Bmatrix}$$

and give the right weight to each sub-category, creating the model equation:

$$y = \begin{bmatrix} \boldsymbol{a} : (\mathbf{1} + \boldsymbol{a_{ir}}) * \{[\mathbf{1} + \boldsymbol{l} * (\mathbf{1} + \boldsymbol{lag})] + [(\mathbf{1} + \boldsymbol{mo} * [(\mathbf{1} + \boldsymbol{cfc}) * (\mathbf{1} + \boldsymbol{mfc}) * (\mathbf{1} * \boldsymbol{emi}) * (\mathbf{1} * \boldsymbol{bfd})]]\} \\ \boldsymbol{t} : (\mathbf{1} + \boldsymbol{t_{ir}}) * \{(\mathbf{1} + \boldsymbol{it}) + [(\mathbf{1} + \boldsymbol{ot} * [(\mathbf{1} + \boldsymbol{tsc}) * (\mathbf{1} + \boldsymbol{hpi}) * (\mathbf{1} + \boldsymbol{thl})]] + [(\mathbf{1} + \boldsymbol{ar} * [(\mathbf{1} + \boldsymbol{lau}) * (\mathbf{1} + \boldsymbol{aic})]] + [(\mathbf{1} + \boldsymbol{fm} * [(\mathbf{1} + \boldsymbol{nfd}) * (\mathbf{1} + \boldsymbol{ntf})]]\} \\ \boldsymbol{s} : (\mathbf{1} + \boldsymbol{s_{ir}}) * \{[(\mathbf{1} + \boldsymbol{em} * [(\mathbf{1} + \boldsymbol{nsi}) * (\mathbf{1} + \boldsymbol{hce}) * (\mathbf{1} + \boldsymbol{hds})] + [(\mathbf{1} + \boldsymbol{rm} * [(\mathbf{1} + \boldsymbol{vam})]\} \\ \boldsymbol{r} : (\mathbf{1} + \boldsymbol{r_{ir}}) * \{[\mathbf{1} + \boldsymbol{fi} * [(\mathbf{1} + \boldsymbol{amy})]\} \end{bmatrix}$$

Description:

- The logical process followed to create this equation implies that risk *(y)* is a multi-components value, which exists in 4 dimensions *(a,t,s,r)*.
- However, each of these variables is shown or not in the investigation of the case *(1 or 0)* and if it shown, it can be in different ways and with different risk impact.
- These different ways translate in the sub-variables that each variable have.
- Each sub-variable however has further different cases in which the scenario can unfold, called sub-categories.

Based on this structure description and the model equation described upwards, we created the scenario model using the decision tree structure.

2.3.1. Decision tree structure: first step

First step to build the binary probability structure was building the decision tree structure, through a simple python model, for all the three layers of scenario.

First thing first I coded the 1st layer and 2nd layer of variables, which accounts for 8192 different nodes that includes all combinations of binary decision.
Then, I built the third layer of the model introducing the sub-categories, first also including the x* variables, meaning the ones that we included on base of literature and contribution of experts, but couldn't test with the sample case study analysis, and then keeping inly the tested variables.
This step of reducing the model only to empirically tested variables, was a necessity to make the model leaner, passing from *137.438.953.472* scenarios, with 24 total sub-categories to *1.073.741.824* with 17.
This structure was built to create a representation of **all the scenario that can happen**.

2.3.2. Case studies: second step

After creating the model infrastructure, to obtain variables values, here we'll describe the case studies analyzed, and the consequent results obtained propaedeutic to variables-values calculations.

1. **Fraud cases:**

a. **FTX Exchange**:

- One of the biggest fraud cases in financial history
- Impact level of 7.

- Damage accounted as $16.000 Mln, but consequences generated for $150.000 Mln of value lost on cryptocurrency market.
- Key variables during investigations included outbound transactions towards shell entities and partners companies such as Alameida, also using the Bahamas location to receive lower tax impact, which is also why they didn't pay any taxes on fund which they also misreported through manipulation.
- Through this scheme they faked liquidity, and assets with their FTT token with no value, used also as leverage for acquisitions, which is a similarity to Wirecard.
- Company never fulfilled regulations within the matter of ICS and failed during AML set of processes.

b. Wirecard AG:

- Biggest recent fraud in Europe, which moved politics and finance in a criminal prosecution on which, Daniel McCrum from FT, one of my contributors, investigated on.
- Impact level of 7.
- Company declared the total absence of $1.900 within its accounts, which was faked by the bank.
- The flags here were in the transactions, both the outbound for acquisitions of indebted businesses, both inbound for bank's acquisitions of "customers portfolio" used, similarly to FTX, as collateral for fraudulent acquisitions with the goal of launder its activities.
- The management lies and their absence of churn compared to the CFO churn, also posed a huge flag during investigations.

c. OneCoin:

- A $4B fraud in cryptocurrency industry, with strong similarities to 1MDB case, where the fund was totally mis-used, criminally, by the managers, and the value of the underlying assets was non-existent.
- Impact level of 7
- Fund misappropriation is a big component in this case, because Ruja Plamenova Ignatova (still searched by FBI) and Karl Sebastian Greenwood (sentenced to 20 years in jail) totally de-frauded investors in Onecoin with fake assets value and market manipulation, which implies the presence of management misreports and cover of fraudulent scheme (mfc)

d. Banco Espírito Santo:

- Sanctioned for $11.800Mln
- Impact level of 7.
- Management total failure and corruption caused in 2014 the bank lost the equivalent of $4.8 billion raising concerns about the health of the bank, and ultimately caused the intervention of Banco de Portugal and liquidation of the bank's activities, seen the state of insolvency, through the development of a bridge-bank that divided the assets in healthy ones in a new bank called NovoBanco, and bad ones in the former BES.

e. Toshiba:

- Fined for $56Mln
- Impact level of 6
- Source of fs elements, especially expenses manipulation paved the way to investigators when discovering that the company overstated pretax profit by 230 billion yen ($1.59 billion) over seven years, but also a strong management fault when between 2016 and 2018 Toshiba tried to cover their $6 billion investment failure.

f. Nissan

- Sanctioned by $2Mln, but generated an impact of 5
- Both source of fs elements and asset location were two red flags present in this case investigation. Carlos Ghosn, the fugitive former Nissan Motor chairperson, was the main figure responsible for hiding his earnings in key securities reports, generating sub-variables flags alert for management & ownership and revenues/assets misreports.

g. 1MDB

- Damage quantified to be $4.5B for a fraud remarkably like FTX, because of fake assets leveraging (FTT Token), to Onecoin, the underlying business was just a cover for management fraud.
- Not only 1MDB inflated and faked wither the value or even the presence of phantomatic assets, creating a false impression of financial strength, but also engaged in off-balance sheet transactions, hiding debt and financial commitments, and diverted company funds to personal accounts, shell companies, and unrelated ventures.
- Relevant parts involved and sanctioned in this case was Goldman Sachs Local Unit which admitted paying bribes to foreign officials and that it had ignored red flags that should have alerted higher-ups to problems with the deal.

h. Carillion

- $7BMln in estimated impact, flagged the assets and transactions red flags
- Impact level of 5
- Resulting in misstatements of more than £800m on Carillion's books, which was totally missed by KPMG auditing

i. Steinhoff International

- Sanctioned with $1.384Mln because Levy and Vinson presented falsely optimistic sales forecasts to Mattress Firm's management to maximize the stores that would be opened and to justify the above-market rents and longer lease terms that were offered to the developers.
- Impact of 7
- Flagged under the revenues/assets misreports sub-variables and acquisitions & restructuring, because of their total sales faking and acquisitions operations through Colliers Atlanta "fixer" role where the company found new business to buy and locations for new openings

2. Corruption cases:

a. RBS GRG

- Loss of $27B, was accused of putting its own interests ahead of its clients when it moved 16,000 small business customers to its Global Restructuring Group (GRG). More than 90% of those customers suffered some form of mistreatment and many were financially ruined between 2009 and 2013.
- Impact level of 7
- Flagged the model with transactions, because of their restructuring policies which they failed to explain to FCA, and many other suspects such reasoning behind decisions relating to pricing and revenue attribution.

b. HP

- Damage of $108Mln
- Impact level of 5
- HP Russia created excess profit margins used to finance management personal expenses. During the investigations they discovered that conspirators inside HP Russia kept two sets of books: secret spreadsheets that detailed the categories of bribe recipients, and sanitized versions that hid the bribes from others outside of HP Russia, turning on the alarm for the source of fs elements flag, but detectable through the outbound transactions and fund fraudulent usage sub-variables.

c. **SBM Offshore**
    - Loss of $238M
    - Impact level of 5
    - Company flagged the model with outbound transaction especially towards high-risk location.
    - During the investigation Office of Public Affairs discovered a scheme involving the bribery of foreign officials in Brazil, Angola, Equatorial Guinea, Kazakhstan and Iraq in violation of the Foreign Corrupt Practices Act (FCPA).

d. **Siemens AG**
    - Fined to pay $1.6B
    - Impact level of 5
    - The executives falsified documents including invoices and sham consulting contracts, signaling a red flag for management & ownership variable, as well as the management fraudulent reporting and Siemens paid more than $100 million in bribes to such high-ranking officials as two former Argentine presidents and former cabinet members.

e. **Huawei**
    - Buggest loss registered in the sample, where the company's actions caused a $39.929 Mln revenue loss attributable to the United States Government company ban on national soil
    - Impact level of 6
    - Based on the official investigation reports, Huawei repeatedly lied to U.S. government about their business in Iran, giving false information to the U.S. Congress, flagging management cover of fraudulent act (subcategory), asset location general risk (lag-subcategory)

f. **Glencore**
    - $1.37B total sanctions for the corruption case
    - Impact level of 7
    - Glencore's has been ordered to pay more than £275m because a subsidiary bribed officials in African countries to get access to oil for a total of $26m to officials of crude oil firms in Nigeria, Cameroon and Côte d'Ivoire.

g. **SNC-Lavalin**
    - $280 Mln of sanction and known as one of the most relevant corruption case in Canadian Parliament

- Impact level of 6
- The case concerns a trip that Al-Saadi Gaddafi took to Canada in 2008—totaling $1.9 million—which SNC-Lavalin paid for, and for which the was detected in the model through high political involvement of the business parties (Canadian politicians) and for the location of transactions parties

h. Gazprom

- $6.5B total loss in fines attributable to corruption accusation over the years, both shell companies' accusations but through Warsaw anticompetition fines against Nord Stream violation of anti-trust violations (regulations fulfillments – variable)
- Impact level of 5

i. JBS

- $128Mln sanction
- Impact level of 4
- Company managers and some of their most senior executives created a vast scheme that involved payments to more than 1,800 politicians, for protection and zero intromission for their acquisitions deals such as the takeover of Tasman Group.
- Flagged under outbound transaction, but also high political involvement and management misreports and cover of fraud

j. Unaoil

- Fined for a total of $ $25Mln
- Impact level of 7
- The company distributed millions of dollars' worth of bribes on behalf of corporate giants including Samsung, Rolls-Royce, Halliburton, and Australia's Leighton Holdings, discovered through leaked files which exposed two Iraqi oil ministers, a fixer linked to Syrian dictator Bashar al-Assad, senior officials from Libya's Gaddafi regime, but also Iran, United Arab Emirates, and Kuwait relevant figures.

k. Odebrecht

- $2.6B total damage
- Impact level of 7
- Executives admitted paying bribes in exchange for contracts worldwide, including Argentina, Colombia, Ecuador, Peru and Venezuela.

l. Petrobras

- $853 Mln for a Bribe scheme, "which took place between at least 2004 and 2012, is estimated at $2bn, of which more than $1bn went to politicians and political parties"

- Impact level of 6

m. Alstom

- $52 Mln fine for Foreign Bribery Charges
- Impact level of 7

3. Money laundering cases:

a. Rabobank

- $367 Mln total damage for allowing illicit funds to be processed through the bank without adequate Bank Secrecy Act (BSA) or AML review
- Impact level of 1

b. NatWest Group

- $265 Mln total sanction for allowing a gold trading business owner who is suspected of having laundered £700K in cash through the group.
- Impact level of 3

c. Swedbank

- Total fine of $386 Mln
- Impact level of 4
- Management agreed to Nasdaq accusation of AML failure.

d. Danske Bank

- Sanction of $2 Mln
- Impact level of 2
- Bank was sanctioned for AML failure which led to illegal money transactions through Banks's branch in Estonia to gain unlawful access to the US financial system

e. Banco Santander

- Fined for $108 Mln for persistent gaps in AML set of processes.
- Impact level of 1

f. N26 Bank GmbH

- Sanction of $14 Mln
- Impact level of 1
- This remains an interesting case because company is more alive than ever now, however the model flagged a strange presence of cross reference for red flags both for regulation fulfillment (AML failure, which caused the multiple sanctions) which in the same period generated also CFO churn while no management churn

g. **Liberty Reserve**
    - Lost their market value for a total of $6B, after they totally faked currency value, and processed at least 55 million illegal transactions for at least one million users worldwide. Fake accounts, domain names flagged the model under shell companies' network, transactions, management fraud covering.
    - Impact level of 7
h. **Credit Suisse**
    - Sanctioned for a total of $2 Mln
    - Impact level of 2
    - Bulgarian drugs transactions made through the bank caused by AML failure, and their client relationship management with OCG's members.
i. **Standard Chartered Bank**
    - Sanction of $1.1B
    - Impact level of 2
    - FCA accused the bank of serious and sustained shortcomings in AML set of processes, which led to violation of Iran's transactions policies.
j. **Deutsche Bank**
    - Sanctioned with $767Mln for the AML failure
    - Impact level of 4
    - Biggest fine arrived from 2017 investigation that discovered connection with a Russian money laundering plan, where bank's clients illegally moved $10 billion out of Russia via shares bought and sold through the bank's Moscow, London, and New York offices.
k. **ABLV Bank**
    - Fine of $3.6B
    - Impact level of 7
    - ABLV Bank received a warning by ECB, who signaled imminent failure because of bank collapsing on its liabilities (source of fs elements > revenue/assets misreports), which started on 2018 a voluntary liquidation plan
l. **Bank of Cyprus**
    - Sanctioned for $2 Mln, for knowingly helped a millionaire, wanted on US soil, to launder profits from an insider trading scheme.
    - Impact level of 2
m. **ABN AMRO**

- Sanction of $480 Mln
- Impact level of 3
- Investigation discovered that three former board members, who it did not name, had been identified as suspects said to be "effectively responsible for violation" of the anti-money laundering act (AML failure > failure in ICS > regulations fulfillment)

n. FBME Bank

- $2.76B total sanction
- Impact level of 7
- The Bank was accused of disguising losses and tax and depreciation manipulation (source of fs elements > expenses misreports) as well as revenue inflating, and fund misuse. A case with strong presence of classic financial statement fraud, however transactions played a huge role in connecting the dots of fraudulent activity, with €43.3 million of undisclosed transactions across multiple joint accounts in 2013 made by Isabel dos Santos, the daughter of former Angolan President José Eduardo dos Santos.

o. Brazil Bank

- $26 Mln sanction, for embezzlement and money laundering accusations with dozens of arrests
- Impact level of 4

(Add bullet points for similarities for cross referencing of variables, subvar, subcat e other)

2.3.3. Variable values: third step

We have the binary model, now we assign values to the scenario through impact ratio calculations of each variable/sub-variable/sub-categories.

1. **Variables Impact Ratio:**
    a. **cross references**: number of cross references between the variable and the others.
    This parameter is **used to assess the relative relevance (rr).**

    b. **% of frequency:** % of cases that shows the variable as red-flag.
    This parameter is **used to assess the general relevance (gr).**

    c. **leading variable risk:** normalized value of frequency as main red-flag.
    This parameter is **used to assess the severity of the variable (sr).**

d. **damage dimension when leading variable:** the generated dimension of damage in cases where the variable was leasing variable
   This parameter is **used to assess the severity of the damage (sd).**

e. **var to cat (corruption) – actualized to impact:** impact of the variable related to the corruption cases it was detected, weighted for the corruption category impact ratio**.**
   This parameter is **used to assess the severity of the variable, related to the corruption category (scc).**

f. **var to cat (fraud) – actualized to impact:** impact of the variable related to the fraud cases it was detected, weighted for the fraud category impact ratio.
   This parameter is **used to assess the severity of the variable, related to the fraud category (sfc).**

g. **var to cat (money laundering) – actualized to impact:** impact of the variable related to the money laundering cases it was detected, weighted for the money laundering category impact ratio.
   This parameter is **used to assess the severity of the variable, related to the money laundering category (scm).**

h. **impact ratio of variable.**
   This parameter is **the result: how the variable impacts on the risk *(y).***

This result called impact ratio, express a value, then multiplied with the various impact of each sub-variables and relative sub-category.
It's a way to give a-priori impact for the presence of this variable, then weighted for the actual risk per each case.

main variable	**impact value of variable**
Assets	0,1438646σ
Transactions	0,6193481σ
Source of FS elements	0,0361250σ
Regulation fulfillment	0,0457237σ

Table 2.3: impact ratio results for each variable

2. Sub-variables and sub-categories:

Sub-variables are affected by the value from the recipient sub-categories.

a. **loan usage in acquisitions (ar) –** acquisitions operations made through loans, totally or partially, which can include financing from banks (debt) or business components such as company's receivables or others.
b. **acquisitions of highly indebted/non ideal companies (ar)** – acquisitions of companies who adds no value to company's operations, often highly indebted or with no apparent significance for operations.
c. **high debt to suppliers (em)** – debt to suppliers also intended as payables, which are registered under current liabilities that derives from advances on payments made by the supplier.
d. **no clear or shady suppliers' identification (em)** – company's supplier cannot be identified or doesn't appear to be known when analyzing their information, but also when decision processes to choose them appears shady or incomplete.
e. **high level of commissions/consultancy expenses (em)** – consultancy or related fees to external figures, when represent a significant share of expenses.
f. **AML multiple sanctions over the years (fi) –** AML failure sanctioned over the years, one or multiple times.
g. **no clear fund usage disclosure (fm) –** company don't provide clear fund usage guidance, or reports doesn't appear to be correct whether assets fund or transaction that haven't been disclosed
h. **no tax paid or applied on fund (fm) –** absence or manipulated company's interest on tax, income tax or taxes paid on company's funds
i. **location of asset general risk (l) –** based on the Basel AML 2023 index, location are considered high risk for values over 6,05 which implies strong risk to incur in a failure of AML processes
j. **board figure/shareholders with clear interest in location with high risk (mo) –** executives, board members or stakeholders with economic interest in location that fall into the category of risk location
k. **CFO churn, or no management churn over v long period (mo) –** Chief Financial Officer of the company that leaves its role as the investigation unfold

or that acted during the period in which the financial crime happened. Management churn is near to zero in these cases.

l. **Management misreported or misguided covering fraudulent schemes (mo) –** incongruences of management misreports, lack of verification of statements, or direct involvement in single or multiple case of AML failure, corruption allegations or fraudulent association
m. **board figure with shady details or not clearly disclosed (mo) –** lack of information about board member's profile, role in the company and/or background.
n. **employees/managers/owner with multiple roles/duties/interest in company network of subsidiaries (mo) –** managers, executives or employees that are involved, in any possible way, with a company that has the role of partner, client, supplier or share interest with the parent company in any possible way.
o. **transactions to/through shell companies (ot) –** transactions that the parent company directed towards network or single shell companies as final transaction party or as intermediary of the final receiver.
p. **highly political involvement of business activities (risk of bribes) (ot) –** company's industry characteristics that make it highly relevant for politics matters, either for the nature of the business or the location where operations are involved
q. **transaction to high-risk locations (ot) –** outbound transactions towards high and max risk location following the Basel AML Index 2023 classification of risk for each country
r. **valuation of assets and revenue manipulations (rm) –** Asset assigned with manipulated value in company's books, and revenue inflated artificially

Given the sub-categories, values is attributed on the standard base of the following calculation which considers each case to attribute to each one of them a different level of risk.
The sub-categories values is obtained following this step:

1. referral case – the case in which the sub-category has been detected
2. sanction and case impact – damage in terms of economics measure and impact classification of the case, previously explained during variables value explanation

Then, based on this variable, for each case is calculated the impact ratio:

1. relevance to case – how much from 1(no significant relevance) to 7(key of the case) the sub-category has been relevant for the case, and for the relative investigation.
2. company dimension – book equity value or market value
3. value (ratio magnitude to relevance) – shows the value of impact both qualitatively (company and brand damage, arrest of managers, social impact) both financially:

$$\frac{sanction}{company\ dimension} * case\ impact * relvance\ to\ case$$

4. value to max – ratio that compares the obtained value to the max reachable value (which is 49)
5. value to max (std) – is a normalization of the value to max. This is a necessary step to align in terms of standard deviation the sub-categories values, to have a final average value for each sub-category
6. impact ratio – result which multiply the normalized value to max to the probability *(p)* of the sub-category, acting as weight on total case. This weight is the percentage relationship between the sub-category and all cases in which it could have been detected (37 – the sample)

In conclusion for each case, and sub-category value, a clear motivation of the relevance to the case assessment is made.

3. Results

We applied the model formula within the sample case of companies, dividing the calculation in three tables: I) Sub-categories value calculated as previously explained, II) Sub-variables binary results, III) Variables binary results and final value

Results show:

1. Risk distribution results skewed towards lower risk values, with 56.7% of companies with a risk between 4.04 and 7.44 (low to medium risk), 27% between 7.44 and 10.84 (medium to high risk), 13.5% between 10.84 and 14.24 and less than

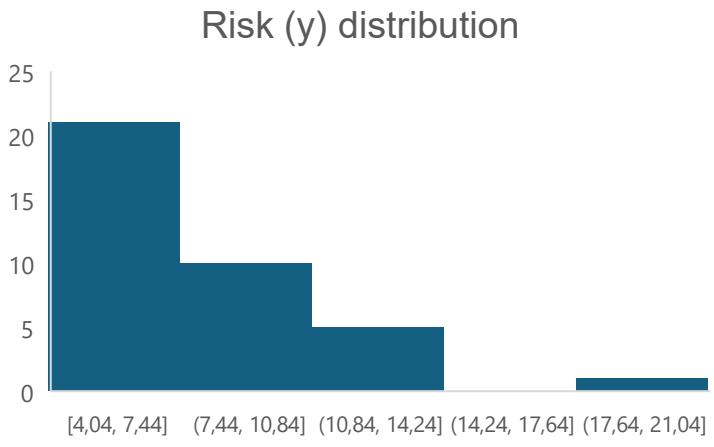

Figure 2.4: risk distribution within the sample

0.1% falling in the tail risk scenario.

2. Testing multiple variables against total estimated risk, transactions results to be the most significant variables, followed by assets. This result is crucial, because in the various experts' contributions, such as Moles from Re-Lender SPA, Nepal from Youngplatform, and as theorized by us during the investigation case information collection, **transactions** was the single variable more present and suspected to be the key variable to identify risk. Assets, the ones with more cross references with transactions, also, has a good correlation with risk, while regulation fulfillments and source of FS elements looks non-conclusive.

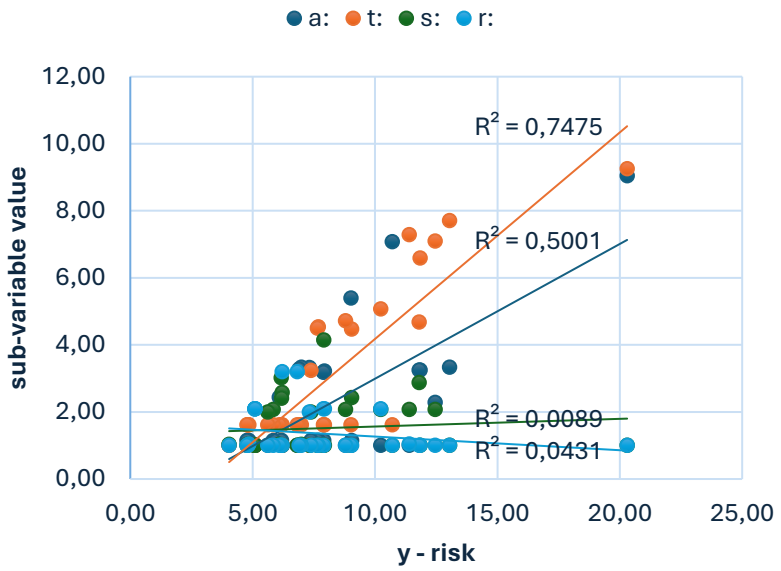

Figure 2.5: variables to total risk contribution – matrix cases

The strong relevance of this key variable is shown when analyzing the relationship of the damage and the contribution per variable:

1st relationship observation: average contribution of t is almost half of total explanation of risk for the cases that generated 66% of total damages, decreasing to 0.32 for the remaining 34% of cases.

% of damage	**65,72%**	**34%**
average t	0,41	0,32
average a	0,23	0,26
average s	0,24	0,21
average r	0,12	0,21

Table 2.4: average contribution to risk by damage categories

2nd relationship observation: to test the proof of transactions as leading risk variable we tested the distribution of the model results, which shows two things:

- on average, the distribution is (as in the 1 results bullet point) skewed towards lower values of risk contribution
- tail risk values show a predominance of transaction contribution

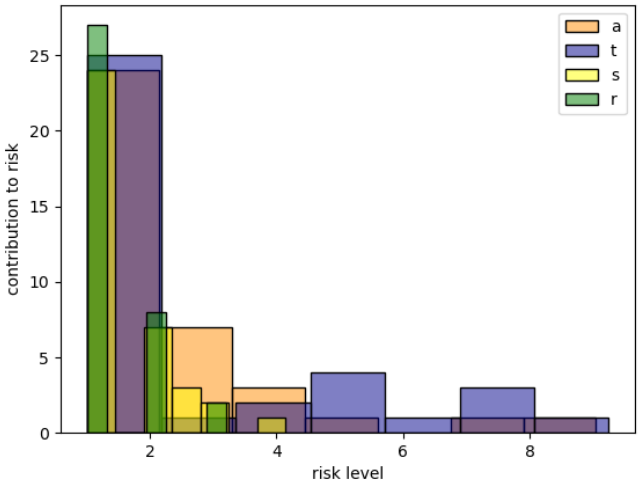

Figure 2.5: contribution to risk by variable

by connecting the **2-relationship observation**, we didn't observe the mere frequency of the variable flagged by the model, but we instead obtained good evidence to assume that **transactions, when found, increase risk expectation.**

3. Corruption and Fraud are the categories of crime with the highest expected damage and impact.
   This information however is only relevant if we understand to which variables those categories are associated.

   The results, also in this case, proves our initial suspect that **corruption risk is strictly related to transactions**,

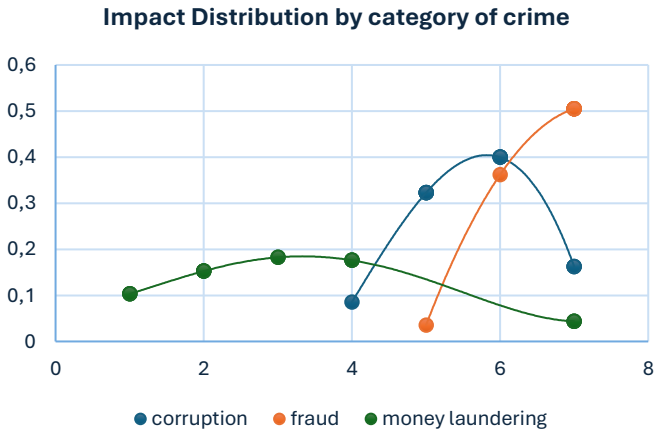

Figure 2.6: impact contribution by category of financial crime

especially to outbound transactions, as the key investigation hints, in corruption cases, are the financial outflows to shell companies owned or connected to politicians or people with relevant authority for company's interests.

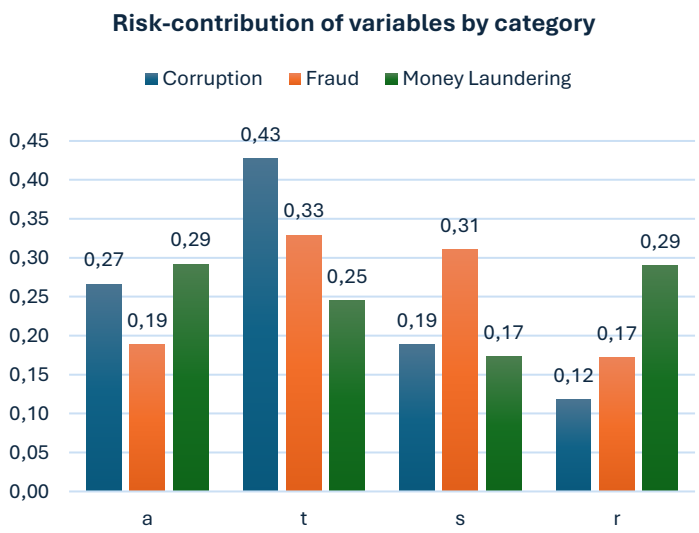

Figure 2.7: risk contribution of variables by category of crime

4. Within the most frequent sub-categories detected, when reviewing the cases of all three categories, by the most frequent ones are:
    a. Management misreported or misguided covering fraudulent scheme *(p=0,38)*
    b. Highly political involvement of business activities (risk of bribes) *(p=0,35)*
    c. Location of asset general risk *(p=0,32)*

    When valuing, other than frequency, also impact to total risk, the results show:
    a. Highly political involvement of business activities (risk of bribes) has the highest impact *(hpi - 0,333167251)*
    b. Location of asset general risk *(lag - 0,306088271)*
    c. Management misreported or misguided covering fraudulent scheme *(mfc - 0,293961616)*

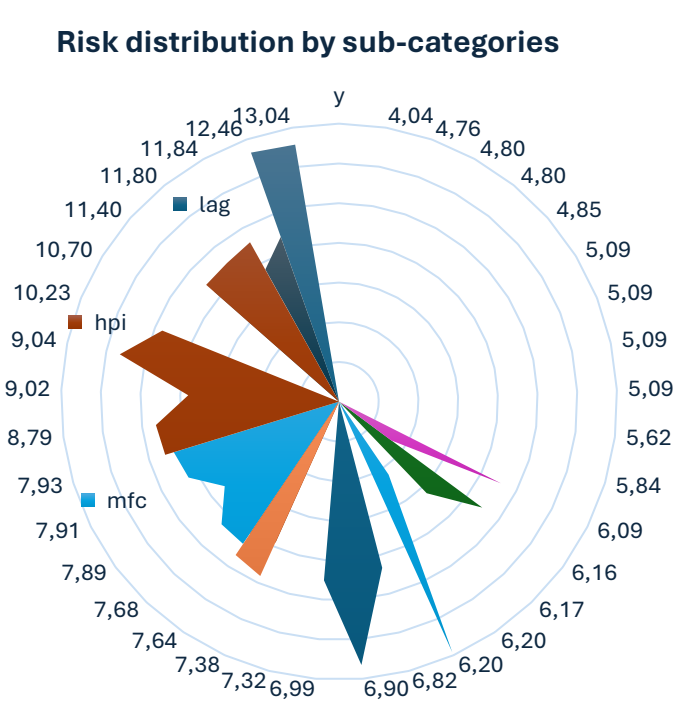

Figure 2.8: sub-categories impact for each case study

subcat	avg impact
hpi	0,33316725
lag	0,30608827
mfc	0,29396162
tsc	0,1045258
hds	0,09893706
thl	0,06659239
cfc	0,06378933
amy	0,05724463
bfd	0,05647768
lau	0,04958315
vma	0,04684812
hce	0,0447892
brf	0,04235428
emi	0,03909376
ntf	0,03473444
nfd	0,03145344
aic	0,02609563
nsi	0,01161043

Table: 2.5: average impact on total risk for each sub-category

Conclusion

Our goal was mainly to find evidence of red flags enabling us to detect financial crimes, and in that case how much those financial crimes weighed on total Eurojust cases.

Results showed that assets, transactions, source of financial statements and regulations fulfillments are the four main concerns of risk valuation within a financial crime, with conclusive evidence of ***transactions*** being the most risk-related factor, with strong emphasis of companies with *high political involvement,* ***assets*** with *location of asset risk*, an indicator based on Basel AML Index, being a significant risk components especially when cross referenced to *outbound transactions* towards *high risk locations*.

The research showed that **corruption cases** are the ones where **transactions** are *most likely to show sign of financial crime*, during **fraud case, source of financial statements** are most useful and during **money laundering cases** the attention should be on (AML) **regulations fulfillment** and **assets.**

The model couldn't be back tested against the counter-proof cases for absence of a well-documented database of companies where no investigation was made.
Results open the door to further research and studies in the context of financial crime prevention and underline the importance for regulators *to* ***focus more on transactions*** *being more transparent and reliable*, understanding that **AML processes** are *easily bypassed*.

References

0) Thesis Database: dati_tesi_manzi.xlsx (to access the database, send an email asking for the password to andreamanzi.work@gmail.com)
0) Thesis Github: amanquant/thesis (github.com)
1) Eurojust reports:
   i. https://www.eurojust.europa.eu/media-and-events/press-releases-and-news
   ii. 2023: https://www.eurojust.europa.eu/annual-report-2023
   iii. 2022: https://www.eurojust.europa.eu/annual-report-2022
   iv. 2021: https://www.eurojust.europa.eu/annual-report-2021
   v. 2020: https://www.eurojust.europa.eu/publication/eurojust-consolidated-annual-activity-report-2020
   vi. 2019: https://www.eurojust.europa.eu/publication/eurojust-annual-report-2019
   vii. 2018: https://www.eurojust.europa.eu/publication/eurojust-annual-report-2018
   viii. 2017: https://www.eurojust.europa.eu/publication/eurojust-annual-report-2017
2) IFAC - 2004. The Auditor's Responsibility to Consider Fraud in an Audit of Financial Statements. ISA 240 (Revised). New York: International Federation of Accountants. 5, par.6
3) PIF: https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/pif-crimes
4) Basel AML index: https://index.baselgovernance.org/ranking
5) FTX
   i. https://www.tradingview.com/symbols/NASDAQ-COIN/financials-statistics-and-ratios/?statistics-period=FY (coinbase – banchmark ratios calculations)
   ii. https://www.coindesk.com/layer2/2022/11/18/a-complete-failure-of-corporate-controls-what-investors-and-accountants-missed-in-ftxs-audits/
   iii. https://www.visualcapitalist.com/ftx-leaked-balance-sheet-visualized/#google_vignette
   iv. https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/
   v. https://x.com/cz_binance/status/1589283421704290306?s=61&t=vqLeym-VZ0uhK9rP8DsqAw
   vi. https://www.riskconcern.com/market-data-and-statistics/asset-turnover-ratio-by-sector-%26-industry-in-the-u.s.
6) Wirecard
   i. https://www.ft.com/content/534e7c4d-3101-3f6a-abc8-dc70beab35b7
   ii. https://www.tradingview.com/symbols/LSIN-0O8X/financials-cash-flow/

iii. https://www.tradingview.com/symbols/LSE-0LVJ/financials-cash-flow/?statements-period=FY&selected=cash_f_operating_activities%2Ccash_f_investing_activities%2Ccash_f_financing_activities%2Cchanges_in_working_capital (benchmarking)
iv. https://viewpoint.pwc.com/dt/us/en/pwc/accounting_guides/business_combination/business_combination__28_US/chapter_4_intangible_US/43_types_of_identifi_US.html
v. https://www.openriskmanual.org/wiki/Accuracy_Ratio#:~:text=Accuracy%20Ratio%20%28AR%29%20is%20a%20summary%20quantitative%20measure,model%20under%20consideration%20versus%20the%20%22perfectly%22%20discriminating%20model

7) Onecoin:
   i. https://www.bbc.com/news/articles/c2llvlx2ez9o
   ii. https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison
8) BES:
   i. https://archive.ph/20240502130455/https://www.reuters.com/article/amp/idUKKBN0G30TA20140804/
   ii. https://it.wikipedia.org/wiki/Banco_Esp%C3%ADrito_Santo
   iii. https://www.novobanco.pt/
   iv. https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-05/cp220076it.pdf
9) Toshiba:
   i. https://finance.yahoo.com/news/timeline-scandal-delisting-toshibas-long-150100732.html
   ii. edgeservices.bing.com/edgesvc/redirect?url=https%3A%2F%2Fwww.asahi.com%2Fajw%2Farticles%2F14872052&hash=hq6Lk9PEVbP0AwIRKtstSs3yWOMLKjSbWliXLoVkG8A%3D&key=psc-underside&usparams=cvid%3A51D%7CBingProd%7C7265AFBC189FB49FF863CCE7974B3E20482136770872EB938E64A534B81035A4%5Ertone%3ABalanced
10) Nissan:
   i. https://asia.nikkei.com/Spotlight/Society/Ghosn-main-culprit-in-Nissan-scandal-Tokyo-court#:~:text=Ghosn%20and%20former%20Nissan%20executive%20Greg%20Kelly%20are,six-month%20sentence.%20Nissan%20was%20fined%20200%20million%20yen
11) 1MDB:

i. https://financialcrimeacademy.org/the-1mdb-money-laundering-scandal-and-corrupt-politicians/#mcetoc_1fg527t7f8
ii. https://www.theguardian.com/world/2015/jul/06/malaysian-task-force-investigates-allegations-700m-paid-to-pm-najib

12) Carillion:
i. https://www.bbc.com/news/business-60243464

13) Steinhoff:
i. https://www.dailymaverick.co.za/article/2024-03-21-steinheist-the-inside-story-behind-the-steinhoff-scandal/

14) RBS:
i. https://good-with-money.com/2017/02/23/rbs-grg-and-what-to-do-if-you-were-affected/
ii. https://www.fca.org.uk/publication/corporate/fca-report-further-investigation-rbs-grg.pdf
iii. https://uk.finance.yahoo.com/news/rbs-grg-smes-fca-final-report-100404724.html?guccounter=1
iv. https://www.spglobal.com/marketintelligence/en/news-insights/trending/jiskjhzcmcyvsqrknwiq2q2

15) HP
i. https://www.justice.gov/opa/pr/hewlett-packard-russia-pleads-guilty-and-sentenced-bribery-russian-government-officials

16) SBM Offshore:
i. https://www.justice.gov/opa/pr/sbm-offshore-nv-and-united-states-based-subsidiary-resolve-foreign-corrupt-practices-act-case#:~:text=SBM%20Offshore%20N.V.%20%28SBM%29%2C%20a%20Netherlands-based%20company%20specializing,violation%20of%20the%20Foreign%20Corrupt%20Practices%20Act%20%28FCPA%29.

17) Siemens AG:
i. https://www.sec.gov/news/press/2011/2011-263.htm#:~:text=Washington%2C%20D.C.%2C%20Dec.%2013%2C%202011%20%E2%80%94%20The%20Securities,to%20produce%20national%20identity%20cards%20for%20Argentine%20citizens

18) Huawei:
i. https://www.bbc.com/news/world-us-canada-58682998

ii. https://finance.yahoo.com/news/huawei-cfo-meng-appear-virtually-125815288.html
iii. https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial

19) Glencore:
i. https://www.bbc.com/news/business-63497376

20) SNCLavalin:
i. https://en.wikipedia.org/wiki/SNC-Lavalin_affair
ii. https://www.ppsc-sppc.gc.ca/eng/nws-nvs/2019/18_12_19.html

21) Gazprom:
i. https://www.themoscowtimes.com/2022/06/16/why-gazprom-corruption-is-bad-for-the-world-not-just-russia-a78012
ii. https://www.politico.eu/article/poland-hits-gazprom-with-world-largest-competition-fine/

22) JBS:
i. https://www.abc.net.au/news/2022-04-25/jbs-meat-company-australia-four-corners-investigation/100997044

23) Unaoil:
i. https://www.offshore-energy.biz/unaoil-says-corruption-allegations-distorted-claims-to-be-victim-of-extortion/
ii. https://www.bbc.com/news/world-58792333

24) Odebrecht:
i. https://www.bbc.com/news/business-39194395#:~:text=Odebrecht%20executives%20have%20confessed%20to%20paying%20bribes%20in,countries%2C%20including%20Argentina%2C%20Colombia%2C%20Ecuador%2C%20Peru%20and%20Venezuela

25) Petrobras:
i. https://www.bbc.com/news/business-45670510

26) Alstom:
i. https://www.justice.gov/opa/pr/sbm-offshore-nv-and-united-states-based-subsidiary-resolve-foreign-corrupt-practices-act-case#:~:text=SBM%20Offshore%20N.V.%20%28SBM%29%2C%20a%20Netherlands-based%20company%20specializing,violation%20of%20the%20Foreign%20Corrupt%20Practices%20Act%20%28FCPA%29.

27) Rabobank:

i. https://www.justice.gov/opa/pr/rabobank-na-pleads-guilty-agrees-pay-over-360-million

28) Natwest Group:
   i. https://www.bbc.com/news/business-59629711

29) Swedbank:
   i. https://www.amlintelligence.com/2021/05/swedbank-handed-fresh-multi-million-euro-fine-for-anti-money-laundering-shortcomings/
   ii. https://www.swedbank.com/investor-relations/the-share/share-statistics.html

30) DanskeBank:
   i. https://edition.cnn.com/2022/12/13/business/danske-bank-justice-department-fraud/index.html
   ii. https://www.reuters.com/legal/danske-bank-pleads-guilty-resolve-long-running-estonia-money-laundering-probe-2022-12-13/

31) BancoSantander:
   i. https://www.bbc.com/news/business-63914275

32) N26:
   i. https://n26.com/en-eu/press/press-release/statement-on-the-fine-issued-to-n26-bank-ag-by-the-federal-financial-supervisory-authority

33) Liberty Reserve:
   i. https://www.justice.gov/opa/pr/one-world-s-largest-digital-currency-companies-and-seven-its-principals-and-employees-charged
   ii. https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital
   iii. https://www.ice.gov/news/releases/charges-filed-against-one-largest-digital-currency-companies-employees-running-6
   iv. https://fastercapital.com/content/Financial-fraud--Liberty-Reserve-Scandal--A-Tale-of-Deception.html
   v. https://insightcrime.org/news/analysis/liberty-reserve-case-exposes-new-frontiers-in-laundering-digital-cash/

34) Credit suisse:
   i. https://www.cnbc.com/2022/06/27/credit-suisse-found-guilty-in-money-laundering-case.html
   ii. https://www.bbc.com/news/business-61957774

35) Standard Chatered Bank:
   i. https://www.bbc.com/news/business-47872318

36) Deutsche Bank:
    i. https://www.justice.gov/opa/pr/deutsche-bank-agrees-pay-over-130-million-resolve-foreign-corrupt-practices-act-and-fraud
    ii. https://www.bbc.com/news/business-38805085
    iii. https://www.bnnbloomberg.ca/deutsche-bank-settles-money-laundering-case-for-7-1-million-1.1794998
37) ABLV Bank:
    i. https://www.lsm.lv/raksts/zinas/ekonomika/asv-par-naudas-atmazgasanu-versas-pret-latvijas-ablv-bank.a267768/
    ii. https://www.lsm.lv/raksts/zinas/latvija/ar-ablv-banku-saistitas-adreses-notikusas-verienigas-kratisanas-aizturetas-vairakas-personas.a3636
38) Bank of Cyprus:
    i. https://www.bankofcyprus.com/ComplianceNewsletter/247-nearly-$1bn-was-issued-in-aml-kyc-and-data-privacy-fines-during-h1-2021/
39) ABN Amro:
    i. https://www.reuters.com/business/abn-amro-settle-money-laundering-probe-574-million-2021-04-19/
40) FBME Bank:
    i. https://www.buzzfeed.com/tomwarren/secrets-of-one-of-the-worlds-dirtiest-banks-revealed
41) Brazil Bank:
    i. https://www.spglobal.com/marketintelligence/en/news-insights/blog/banking-essentials-newsletter-july-10th-edition

words count: 7753