ACUMINOR SERIES 1

Implementing an intelligence-led approach across your financial crime framework

A THREAT-LED APPROACH TO FINANCIAL CRIME PREVENTION

What does it mean to be Threat-led in your approach to financial crime prevention, and why it is important?

ACUMINOR

"TO PROTECT YOUR ORGANISATION AND WIDER SOCIETY FROM THESE THREATS, YOU NEED TO UNDERSTAND WHICH THREATS ARE RELEVANT TO YOU, HOW THOSE THREATS MANIFEST IN YOUR ORGANISATION AND WHAT YOU CAN DO ABOUT THEM THIS IS THE THREAT-LED APPROACH."

EXECUTIVE SUMMARY

Threats occur in the real-world, they involve real people – perpetrators, victims, enablers, insiders - and many other people and objects that get caught up as collateral damage. Each threat may involve multiple modus operandi (or methods for committing a crime), some methods change and evolve significantly, while some remain pretty much the same.

In the context of financial institutions, threats can be thought of as the ways in which your organisation can be misused for money laundering, terrorist financing or sanctions evasion purposes.

To protect your organisation and wider society from these threats, you need to understand which threats are relevant to you, how those threats manifest in your organisation and what you can do about them. This is the threat-led approach.

There are three levels of intelligence relevant to financial crime risk: strategic, tactical, and operational. We will dive into these three levels in more detail in a future paper. But here, you can think of intelligence as deep knowledge about the financial crime methods that could impact your organisation in an ever-changing world. Today, most organisations don't have the intelligence they need to implement a true threat-led approach. Due to this missing information, organisations are forced to jump to conclusions about their customers, countries of operation, products, and transactions, without knowing the real-world reason why these people or movements of money may be risky, and which real-world threat they are related to.

Implementing a threat-led approach successfully gives an organisation the opportunities to re-calibrate their financial crime framework. Using a worked example, this technical paper will explain how focusing on threats first, and risk second, will allow you to meaningfully reduce the volume and value of financial crime affecting your organisation.

"A COMBINATION OF THESE FACTORS HAS MADE HORIZON SCANNING FOR THREATS AND RISKS AND KEEPING ON TOP OF THE VAST QUANTITY OF EVOLVING SOURCES AND INFORMATION, AN ALMOST IMPOSSIBLE TASK. MUCH OF THE INFORMATION THAT IS PUBLISHED, FOR EXAMPLE IN COUNTRY NATIONAL RISK ASSESSMENTS, IS UNSTRUCTURED. MEANING IT'S HARD TO DIGEST THE INFORMATION AND MAKE THE LEAP TO DETERMINE WHICH PARTS ARE RELEVANT FOR YOUR ORGANISATION, CUSTOMERS, AND PRODUCT OFFERING."

WHY IS IT HARD TO FOCUS ON THREATS?

Knowledge of financial crime threats must be disseminated across the entire financial ecosystem to encourage a concerted and coordinated effort to prevent illicit activity. Today however, information about financial crime threats is often hidden in unstructured free text, such as government or law enforcement reports and isn't shared consistently. Without a clearly defined taxonomy that translates threats into financial crime risk indicators, the information held within financial crime typology, or 'red-flag' reports has limited value.

Much of the intelligence on financial crime typologies is shared informally between a handful of individuals at closed events or via email. Conversations within and between relevant organisations are ongoing during investigations, but many partnerships lack the required frameworks to store, share and update the modus operandi that can be gleaned from a tactical investigation. Static information on threats does little to enable firms, regulators, and law enforcement agencies to keep pace with organised crime groups, and the same modus operandi are exploited by criminals over and over again.

A combination of these factors has made horizon scanning for threats and risks and keeping on top of the vast quantity of evolving sources and information, an almost impossible task. Much of the information that is published, for example in country national risk assessments, is unstructured. Meaning it's hard to digest the information and make the leap to determine which parts are relevant for your organisation, customers, and product offering.

WHY IS IT IMPORTANT TO FOCUS ON THREATS?

If you agree that measuring effectiveness in financial crime mitigation should mean 'how well are you tackling your actual risks (not your perceived risks) in an ever-changing world?' then you will agree we need a way for organisations to record what their actual risks are. To gain insight into these real risks, you need to first understand threats in the real world first and then how those break down into risks that could impact your organisation.

Historically this hasn't been possible since organisations have not had the necessary data available nor a workable structure and taxonomy to implement an evidence-based threat-led approach. Today, horizon scanning often falls to internal experts who use their knowledge and industry experience to document threats and risks. Despite this knowledge being highly valuable, there is room for error due to reliance on unstructured sources, inconsistent intelligence streams, alongside manual out-dated approaches and competing resource demands. Over-reliance on human expertise also leaves organisations open to biases. For example, if one individual has lots of experience in one particular modus operandi or a particular organisation has filled multiple SARs for one modus operandi – they could be more likely to look for that type of behaviour going forwards. On top of this, your internal experts may move on to new jobs, taking knowledge with them and this makes it extremely hard to have a resilient approach.

"THREATS GIVE YOU THE CONTEXT AS TO WHY SOME RISKS ARE RELEVANT FOR YOUR ORGANISATION AND OTHERS AREN'T. APPLYING THIS THREAT LAYER GIVES YOU A VERY STRONG RATIONALE AS TO WHY YOU HAVE DECIDED TO PRIORITISE SOME RISKS OVER OTHERS. BY USING A THREAT- LED APPROACH, YOU CAN ALSO QUANTIFY WHY CONTROLLING SOME RISKS WILL HAVE A GREATER IMPACT ON THE EXTERNAL THREAT ENVIRONMENT THAN OTHERS. THIS APPROACH MEANS THAT YOU CAN DRIVE YOUR ACTION PLAN AND FINANCIAL CRIME PRIORITIES BASED ON OBJECTIVE FACTS."

WHY IS NOW THE TIME TO IMPLEMENT A THREAT-LED APPROACH?

Technology is changing the threat intelligence landscape. It is now possible to systematically understand the threats you are facing, determine how those threats impact your business and understand how well your control environment is doing at mitigating the threats you face.

Supervisory approaches are increasingly data-led and supported by greater cooperation internationally. Failure to oversee your control framework with sufficient rigour whilst ensuring this is proportionate to the risks you face, has led to regulatory action and this continues to demonstrate the importance of a well-defined business wide-risk assessment methodology.

When it comes to implementing a 'risk-based approach' firms are still struggling to define what a risk is and to evidence why certain risks are higher priority than others. This is because they are missing the threat layer. Threats give you the context as to why some risks are relevant for your organisation and others aren't.

Applying this threat layer gives you a very strong rationale as to why you have decided to prioritise some risks over others. By using a threat-led approach, you can also quantify why controlling some risks will have a greater impact on the external threat environment than others. This approach means that you can drive your action plan and financial crime priorities based on objective facts.

A combination of technology enablement and regulatory pressure suggests that the time is now to move your organisation towards a threat-led approach. The following worked example shows you how this can be achieved.

Implementing a threat-led approach successfully gives an organisation the opportunities to re-calibrate their financial crime framework. Using a worked example, this technical paper will explain how focusing on threats first, and risk second, will allow you to meaningfully reduce the volume and value of financial crime affecting your organisation.

"AT THE TIME OF WRITING ACUMINOR HAD ANALYSED 750 FINANCIAL CRIME REPORTS, TOTALLING MORE THAN 300 000+ PAGES TO CREATE A DATABASE OF 3 000 THREATS AND 11 000 RISK INDICATORS. IF YOU WERE TO RE-CREATE THE SAME ANALYSIS MANUALLY IT WOULD TAKE YOU 100 000 HOURS OR APPROXIMATELY 54 YEARS WORKING FULL TIME."

A WORKED EXAMPLE – IMPLEMENTING A THREAT-LED RISK ASSESSMENT

Since 2018, Acuminor have been on a mission to re-think how organisations identify and assess financial crime threats and risks. This worked example looks at how a financial institution can create a threat-led risk assessment using Acuminor's Risk Assessment Pro Platform and a threat-led methodology.

Step 1: Understand the threats facing your organisation – an intelligence driven approach

Understanding the threats your organisation faces requires an analysis of the external environment. Acuminor collects financial crime intelligence from a vast number of vetted sources. Experts, assisted by technology together with machine learning models, process significant volumes of information, structuring this into the intelligence behind Acuminor's comprehensive library of threat and risk indicators.

At the time of writing Acuminor had analysed 750 financial crime reports, totalling more than 300,000+ pages to create a database of 3000 threats and 11,000 risk indicators. If you were to re-create the same analysis manually it would take you 100,000 hours or approximately 54 years working full time.

Acuminor's intelligence is organised on a global, regional, and national level. Structuring the intelligence in this way allows for a systematic approach to analysing the threat landscape and standardises the taxonomy for threats and risks so that you and your organisation can draw evidence-led conclusions about how financial crime can impact your operations in different countries.

Acuminor studies the relationships between threats and risk indicators to make the link between each individual risk (e.g., a particular transactional risk) and the threats that risk indicator is associated with. Studying and presenting financial crime intelligence in this way highlights the unique profile of each threat and the many possible connections and relationships between threats and risks. There are thousands of many-to-many connections in the database, far too many to do a comparable analysis manually, especially in the time typically allocated for an annual risk assessment.

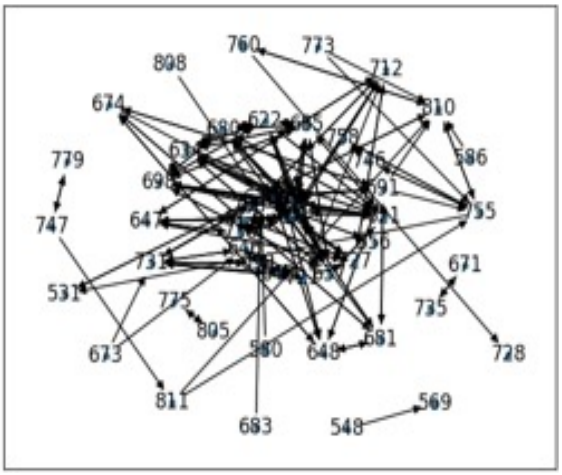


Figure 1: A depiction of the many-to-many connections between risk indicators within Acuminor's database

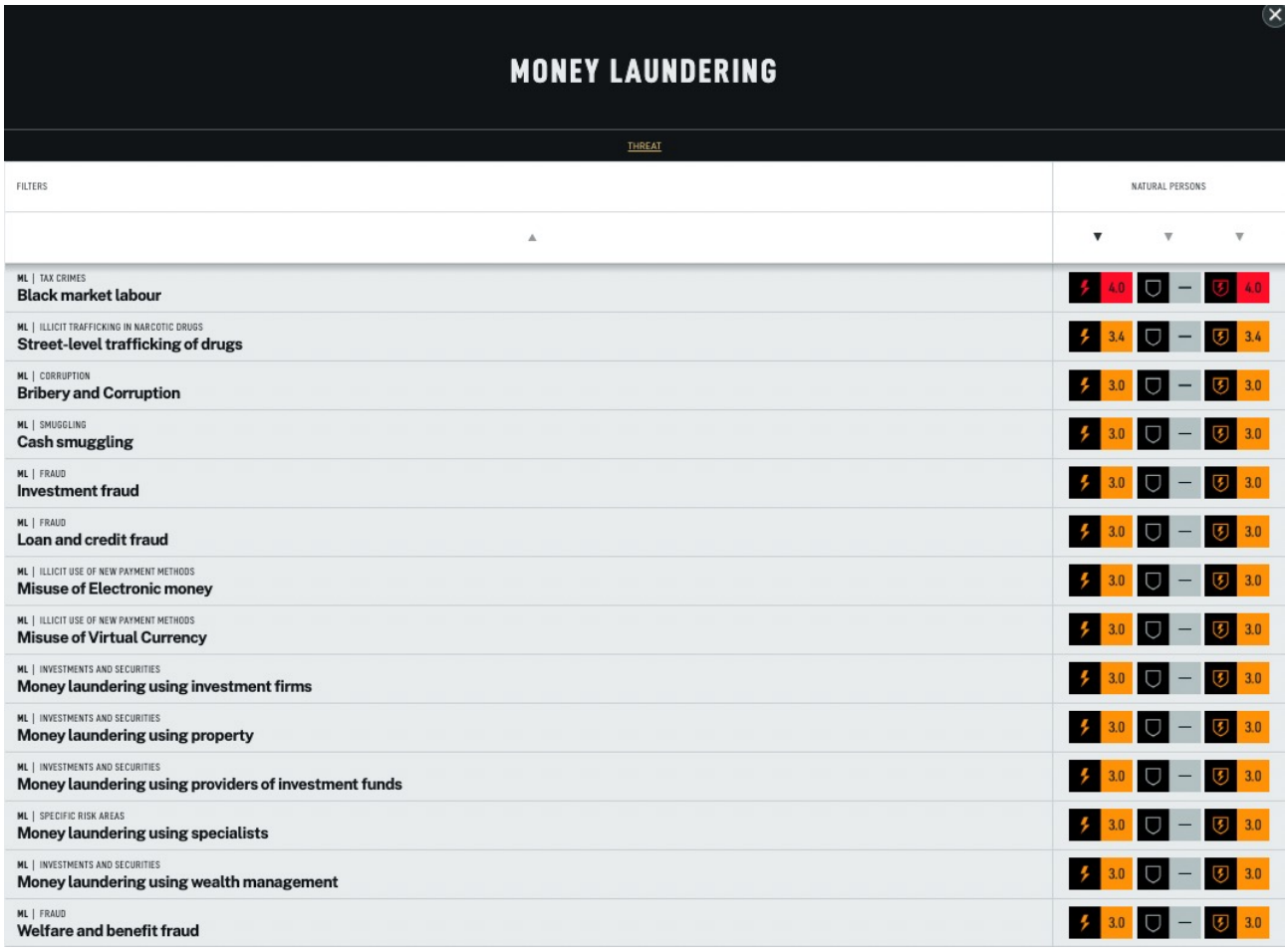


Figure 2: A selection of inherent threats pulled form Acuminor's fincrime intelligence database -inherent risk for threats
From left to right the scores show, inherent risk, control strength, residual risk.

All threats and risks are tagged in Acuminor's database, this means that an organisation can search across the database to see which threats are relevant for their customers, products, channels, and geographies.

In this case, Acuminor's platform shows that there are 49 threats relevant for this example financial institution.

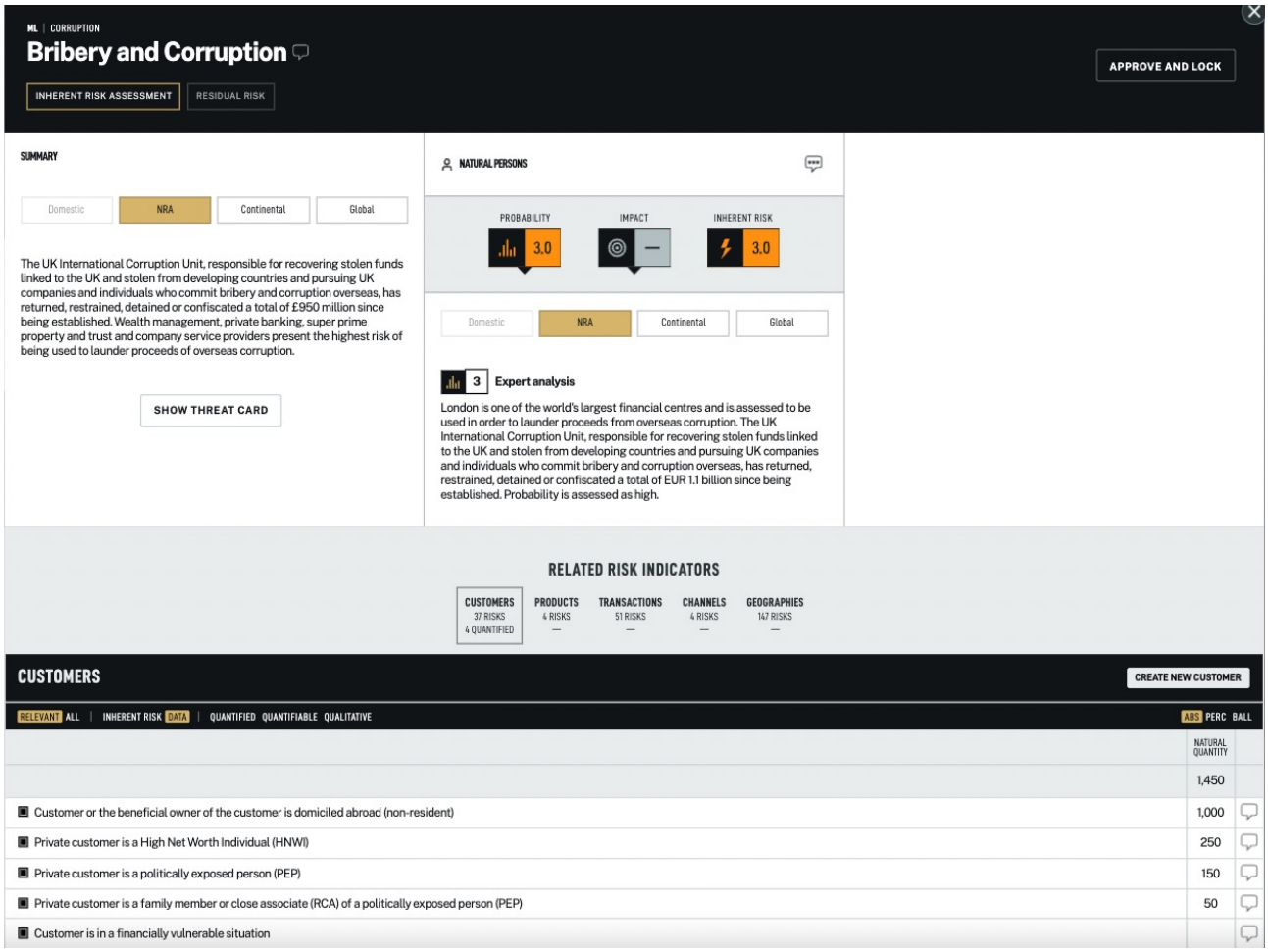


Figure 3: A demonstration of how one threat (here Bribery and Corruption) can break down into multiple risk indicators

Step 2: Understand how the relevant threats impact your operations

Each threat breaks down into many risk indicators across the 5 key risk categories: customers, products, transactions, channels, and geographies. Some risks can be quantified, to help this organisation understand how exposed they are to each threat.

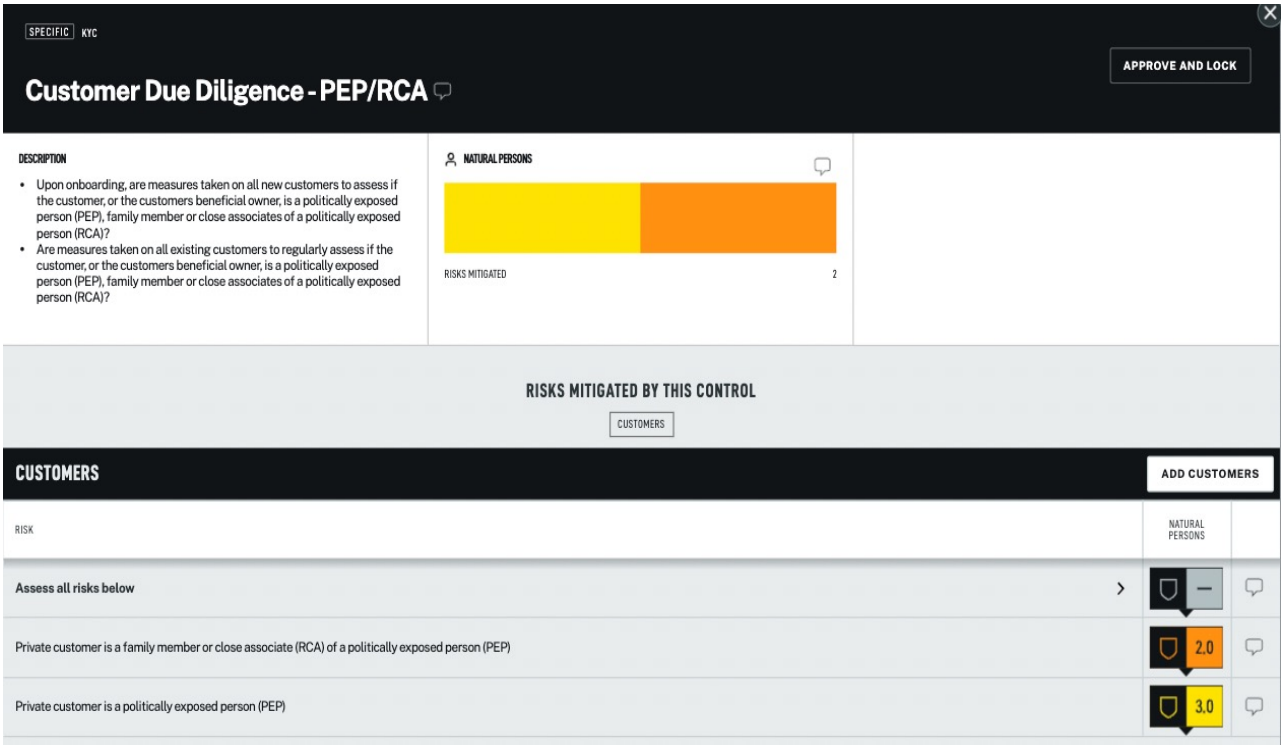


Figure 4: An example of linking a control to the risks it is mitigating and scoring the effectiveness of the control at that level.

Step 3: Apply controls to mitigate your risks and threats

To measure the effectiveness of controls, an organisation implementing a threat-led approach should ask itself three questions:

1. **What controls do we have?**
2. **Which risks are the controls mitigating?**
3. **How well do the controls perform?**

By framing control design and effectiveness in this way, an organisation can ensure that they are focussed on what they can do about real risks and the knock-on impact this has on real world threats. Once they have linked all their current controls to the risk these mitigate, (because those risks are linked back to threats), it follows that they will then be able to understand how well they are doing at tackling their threat landscape.

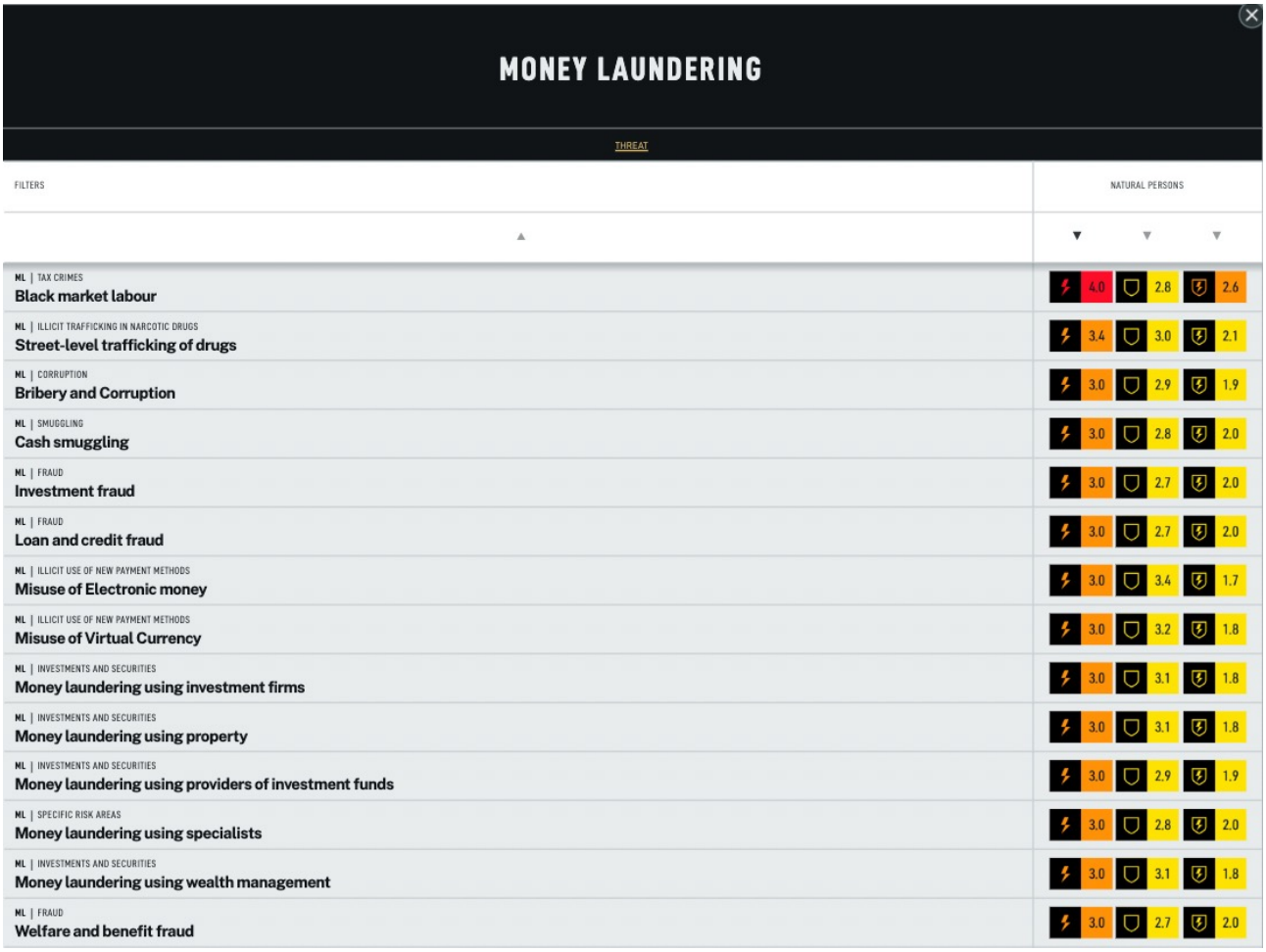


Figure 5: A demonstration of how effective threats are being mitigated – residual risk for threats
From left to right the scores show; inherent risk, control strength, residual risk

Step 4: Review how well financial crime controls are performing against the threat landscape

Once an organisation has assessed their existing controls, they can then visualise how effective these controls are at mitigating their relevant threats.

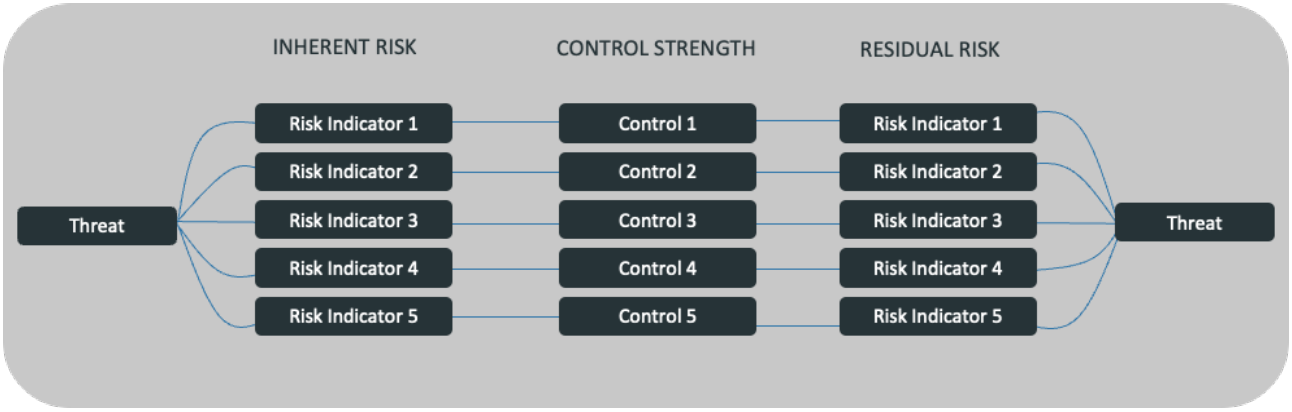


Figure 6: : An overview of the threat-led methodology

A summary of the threat-led methodology

This worked example has demonstrated that it is now possible to implement an intelligence-led & threat-led approach to your financial crime risk assessment. It takes a huge volume of structured and mapped financial crime intelligence to make this possible.

A particular threat is determined as relevant or not relevant based on a systematic digestion of official sources of financial crime intelligence. Each threat breaks down into multiple risk indicators. Controls are then linked to the risks they mitigated and scored for effectiveness which drives the residual risk score for each threat.

"IMPLEMENTING A THREAT-LED APPROACH WILL ALLOW AN ORGANISATION TO TRANSFORM THEIR ENTIRE FINANCIAL CRIME FRAMEWORK TO FOCUS ON MITIGATING REAL WORLD THREATS"

'THE WHY' – WHAT ARE THE BENEFITS OF IMPLEMENTING A THREAT-LED APPROACH?

Implementing a threat-led approach will allow an organisation to transform their entire financial crime framework to focus on mitigating real world threats.

The key benefits of implementing a threat-led risk assessment:

1. Focus on objectively documented criminal activity instead of relying only on internal expertise

2. Concentrate on your highest risks, allowing you to allocate resource efficiently across the financial crime framework

3. Identify the controls which have the highest impact on your threats and risks and improve governance and oversight over changes proposed to this, quantifying the impacts of these.

4. Empower staff to do more of the job they signed up for.

5. Implement a consistent language both internally and externally - improve understanding and awareness of real-world threats, evolving maturity and a risk aware culture

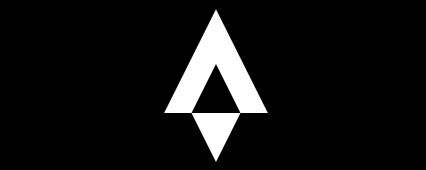
6. Improve your ability to detect and report to regulators and law enforcements agencies whilst also managing your exposure to risk in line with risk-appetite.

7. Limit unnecessary de-risking often caused by lack of resource, misunderstanding the threat and risk landscape or due to a poorly mapped control environment - empowering your organisation to adopt a truly risk-based approach.

A call to action – get in touch to implement a threat-led approach

If you'd like to implement a threat-led approach and improve the outcomes of your entire financial crime programme, get in touch with us at:

sales@acuminor.com



A BRIGHTER WORLD

Sveavägen 140
113 50 Stockholm
SWEDEN

1 Poultry
London EC2R 8EJ
UNITED KINGDOM

acuminor.com
+46 8 121 586 30
relations@acuminor.com