The Wolfsberg Group Frequently Asked Questions (FAQs) on Negative News Screening

Introduction

Conducting searches for “Negative News Screening” (NNS) and other forms of adverse information enhances Financial Institutions’ (FIs’) awareness of potential Financial Crime risk posed by both existing and prospective customers. While there remain some limitations and challenges pertaining to broad media searches, NNS can be a valuable mechanism which enables FIs to have a better understanding of who they are doing business with and the risks to which an FI is exposed.

Although the Financial Action Task Force (FATF) do not explicitly refer to NNS, reference to conducting “adverse media searches” through verifiable adverse media can be found in their Risk-Based Approach Guidance under ‘Enhanced Due Diligence measures’ section[1].

There is no single, universally agreed approach to NNS, therefore the Wolfsberg Group (the Group) has developed this Guidance to assist FIs in establishing their NNS framework in support of Financial Crime Risk Management.

NNS should not be confused with other forms of searches such as Sanctions or Politically Exposed Persons (PEP) screening, which are traditionally list-based. The Group has published separate guidance papers on both topics[2]. This document seeks to articulate relevant considerations which FIs may find useful in setting out NNS standards with consideration to:

- Applying NNS as part of a risk-based approach to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF).
- Documenting a risk-based approach to NNS, taking into account the legal and regulatory requirements in the jurisdiction(s) in which the FI operates.
- Ensuring that NNS processes are both effective and efficient.

[1] FATF, “*Guidance for A Risk-Based Approach*”

[2] The Wolfsberg Group “PEP Guidance 2017”, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/4.%20Wolfsberg-Guidance-on-PEPs-May-2017.pdf and “Sanctions Screening Guidance 2019”

Furthermore, the document also provides guidance on assessing the reliability of NNS sources and the materiality of NNS results as well as the configuration of screening systems, alert management, and associated governance.

This document focuses on FIs which apply NNS to their customers in order to assess the customer's risk profile. While the focus of this paper is mainly on the use of an automated screening tool, FIs that conduct manual searches may still find it relevant. It is important to acknowledge that NNS should not be a zero-tolerance process and that FIs may conclude that NNS is not necessary in all circumstances. It is not intended to suggest all FIs should apply all NNS elements to the same level, rather, it attempts to guide users through the process of establishing an effective risk-based approach to the screening of customer names against adverse information.

Risk-Based Approach and Negative News Screening

There are numerous references to the risk-based approach (RBA) throughout this document. Adherence to risk-based standards is paramount to applying a proportionate approach to NNS and effective and efficient risk management. The Group recommends reading this document in conjunction with its Guidance on the Risk-Based Approach[3] and, as required, other applicable guidance issued by authorities in the jurisdiction(s) in which a FI operates.

Q1. What is Negative News?

The Group recognises that there is no universally agreed and accepted definition of Negative News. For the purpose of this document, it has been broadly defined as 'information available in the public domain[4] which FIs would consider relevant to the management of Financial Crime risk'. Negative News is also referred to as Adverse Media, Negative Media or Adverse News.

Q2. Why might an FI conduct Negative News Screening in the context of fighting Financial Crime?

Conducting searches for Negative News and other forms of adverse information can enhance an FI's awareness of potential Financial Crime Risk posed by existing and prospective customers. It can be a useful screening mechanism which enables FIs to have a better understanding of who they are doing business with and the risks to which an FI is exposed.

NNS enables an FI to leverage a range of information, data, and analysis available in the public domain and can be a useful tool to supplement the Customer Due Diligence (CDD) process and identify factors which may impact on the risk profile of the Customer. This can assist an FI understand the Financial Crime and related Reputational risks posed by a business relationship so that they can be managed appropriately.

Q3. How might NNS add value in fighting Financial Crime?

The Group believes NNS can add value to a Financial Crime Risk management strategy in several ways:

- Revealing involvement in criminal activity which may determine the need for additional due diligence and/or targeted reviews of past transactional activity to inform the decision to on-board, maintain or exit a relationship.
- Informing the risk assessment and classification of the customer or business relationship and determine the extent of ongoing monitoring.

[3] Wolfsberg Statement, *Guidance on a Risk-Based Approach for Managing Money Laundering Risks*
[4] Public Domain: media sources from online news outlets, court records, regulatory disclosures, penalty notices.

- Forming a key component of a CDD trigger event strategy resulting in the more effective deployment of resources.
- Providing additional context to support an investigation into potentially suspicious activity, which may itself be triggered initially by the identification of Negative News.
- Forming an integral element in constructing and identifying potential risks or controversies with respect to a customer's source of wealth and/or source of funds narrative.

Q4. How can an FI ensure NNS adds value without the need for excessive manual resources?

In all cases, an FI should adhere to a risk-based approach with respect to the performance of NNS. Based on an assessment of the risk and the value an FI will derive from NNS, the FI should determine, for example, the extent, timing, and configuration of screening to be performed. FIs should configure their approach to optimise effectiveness, considering the likelihood of identifying a risk-relevant productive alert/true match[5].

The value an FI is able to extract from NNS is correlated to the availability of information and the credibility of the media source in the public domain. For example, customer types such as High Net Worth individuals, PEPs and Institutional customers (Large Corporates and FIs), are more likely to have a high public profile, and therefore, would be expected to be subjected to a higher degree of media scrutiny of both a positive and negative nature. In these situations, the performance of broad based ('structured' and 'unstructured'[6] sources) NNS may be appropriate on a risk sensitive basis. On the other hand, a typical retail or mass-market customer will likely have a lower public profile and therefore much less media scrutiny of either a positive or a negative nature. In this instance, more targeted searches of structured news and media sources might be more appropriate to ensure an effective use of resources. It may also be appropriate not to conduct NNS; an FI would not be expected to devote resources to NNS where the added value is negligible or disproportionate to its Financial Crime Risks. Consideration should be given to whether alternative measures such as anti-fraud databases provide more effective means of risk identification.

Q5. What factors might an FI consider when establishing NNS?

Typically, there are two key factors to consider when establishing NNS. First, FIs should determine the risk categories to screen e.g., the types of crime or event in scope of NNS. The second factor is the 'maturity' / stage of the crime or event committed:

- **Risk Category**: For example, the predicate offence the FI wishes to screen in the scope of its NNS solution e.g., Money Laundering, Terrorism/Terrorist Financing, Bribery and Corruption, Organised Crime, Drug Trafficking, Human Trafficking, Wildlife Trafficking, Proliferation and Proliferation Financing, and Tax Evasion.
- **Risk Stage**: This is the maturity of the offence and starts with an allegation, which then likely becomes an investigation which may lead to charges ending with a conviction. An FI will need to determine at which stage it wishes to be alerted to the potential Negative News, recognising that alert volumes at the allegation stage will be higher than receiving an alert at conviction stage once the alleged crime has been investigated and may have less AML/CTF value.

[5] Refer to the Wolfsberg statement on Demonstrating Effectiveness

[6] in this context, structured data refers to tailored article data that may be narrowed to focus solely on risk relevant information, for example, through the selection of specific offence types/media sources. Conversely unstructured data represents unfiltered raw data that when utilised in the NNS process will typically return much broader outcomes.

The categories of offences, as well as stages of crime, may be subject to local legal definition which FI's need to consider while defining their risk framework.

Q6. What information might be excluded from NNS?

An FI should ensure that Financial Crime related Negative News is distinguished from other Negative News which is not considered relevant. For example, civil proceedings may be excluded from NNS, e.g., speeding fines and public disorder offences which are not related to Financial Crime. This is at the discretion, and in line with the risk appetite of each FI.

Q7. What is meant by the term Reputational Risk in the context of Financial Crime NNS?

Reputational Risk in the context of Financial Crime NNS relates to the risk of negative public perception with respect to the FI's association with a customer or business relationship which may or may not be relevant from a Financial Crime perspective.

By its very nature all Financial Crime Negative News may also pose a Reputational Risk and should therefore, also be considered through such a lens. However, it is acknowledged that while the FI maintains a degree of control in the management of its Financial Crime Risk, Reputational Risk, to some extent is beyond the control of the FI as it varies significantly based on what is of interest to the public and/or according to culture and geography.

For example, an FI considering a relationship with a new corporate customer, may identify Negative News relating to allegations of Money Laundering or Terrorist Financing by the Ultimate Beneficial Owners (UBOs) of the entity. Following an Enhanced Due Diligence (EDD) process, the FI may satisfy itself that the allegations are false, and that the entity is owned and controlled by individuals of sound reputation and standing. On this basis, the FI would also be able to demonstrate and explain, where necessary, the steps it had taken and the basis on which it accepted the relationship. However, it would not necessarily be able to mitigate the Reputational Risk in the same manner. The Reputational Risk element should therefore be assessed and considered in its own right and any decision taken accordingly by the relevant risk owner(s).

Q8. Which relationships might be in scope of an FI's NNS?

Typically, FIs will focus NNS on customers and business Relationships. In line with their risk appetite, FIs may elect to broaden the scope of NNS, e.g., vendors or third-party suppliers.

Q9. What factors might be considered by the FI when determining the scope of NNS performed?

Each FI's approach to NNS should be commensurate with its size, geographical presence, business and technology environment. NNS can be conducted through a variety of approaches, such as batch screening[7], manual screening or real-time screening[8].

Factors to consider when determining the manner in which NNS will operate include, amongst others, the customer risk rating or customer type. Consideration should also be given to the following risk factors:

- the products a customer uses
- the segment to which the customer belongs
- the geographies where the customer is based or to which they have a nexus

[7] An automated screening process eliminating manual input of individual or entity names Screening at periodic intervals provisioning alerts for review at a set time

[8] Screening against a live data source

- the status of the customer’s internal risk rating or score, which may incorporate the above elements
- the inherent risks and financial crime threats applicable to the FI’s business segments.

Q10. What Risk-Based decisions may an FI need to consider in the context of NNS?

While there is no one-size-fits-all approach, the following considerations can help all FIs to determine areas of focus for effective risk management. The Group believes that each category stipulated below should be tailored to an individual FI’s risk appetite.

Risk-based decisions may include:

- Type of Screening: e.g., performing this manually, the use of internet search engines or automation through an internally or externally built solution. It could also be a combination of all of these.
- Scope of Screening: an FI’s CDD/EDD process and technology should determine who should be screened (e.g., customers, UBOs, related parties or non-customers).
- Frequency: an FI will need to determine at what frequency and stage of the customer life-cycle screening should take place (e.g., daily, weekly, monthly, quarterly, annually, whenever CDD/EDD is conducted, including onboarding, triggered event, periodic, on-going basis).
- Media Sources/Lists: an FI may establish specific media sources to be in-scope of monitoring (e.g., consideration can be given to the credibility of the source, and the coverage of adverse information within a specific geographical span).
- Risk Categories and Stages: as referenced in FAQ 5.
- Timelines: an FI may establish a period of how far back media should be screened for the in-scope risk categories. A multi-year look-back threshold may be appropriate, either for all media or higher or lower periods based on the crime/offence types. Additionally, once an initial review has been conducted (e.g., at onboarding) it may only be necessary to screen against new media events.
- Alert filtering criteria:
    - The use of conditional screening rules using list data or source data attributes such as geography location matches or Date of Birth tolerances, (e.g., +/- 1 year).
    - The use of screening solutions where the full range of data is screened or only the data that has changed since the last screening (the delta).
    - Auto Discounting – use of rules designed to manage common false positive alerts eliminating unnecessary manual review.
- Data Purge: removal of reference data from screening once the data is no longer risk-relevant or a former customer relationship is no longer required to be screened.
- Operating Model:
    - Policies and procedures
    - Alert Management
    - Training
    - Quality Control and Quality Assurance
    - Governance, including Management Information

Q11. Screening in multi script languages can be challenging, what are the Key Terms used?

- Transliteration: is the process of transferring words written in one language script to another similar-sounding script enabling pronunciation in another language (e.g., 歌川豊春 <> Utagawa Toyoharu).

- Transcription: is the process of transferring words written in one language script to another in accordance with a certain conversion system. Transcription methods can vary greatly, therefore one word or name can be transcribed to its different variations or ordering depending on language phonetic systems and transcription method (e.g., Piotr Czajkowski <> Pyotr Tchaikovsky <> Piotr Chaykovskiy).
- Translation: is the process of rendering the meaning of the text in another language (e.g., أبوظبي <> Abu Dhabi).

Q12. Does an FI need to conduct NNS in multi script languages?

Depending on the geographical location of the FI or markets where the FI is present, there could be a need to screen the names of customers in the respective local language depending on local regulatory requirements and/or perceived additional risk-effectiveness that such screening could bring. In order to achieve effective screening in a local language, FIs should consider the following:

- The screening system capability to support non-Latin character sets.
- Whether the media sources and customer datasets used by the FI contain the names and Negative News in the native script of that country.

In the absence of the second point, the screening filter should be able to transliterate the customer names from native script to Latin characters and for the filter system to be able to carry out the screening against the media sources in Latin characters.

For FIs that do not purchase media sources from data service providers, it is recommended that the appropriate local teams should be given responsibility to source such media articles and gather this information for screening. Consideration should be made to the documentation defining the rationale for source inclusion/rejection.

Overall, multi-language screening is a challenging area. Where it is a regulatory requirement to perform NNS, consideration must be given to the screening tools available and the associated language capability. This consideration should include the availability of both input and media source data being in the same native script, or the input data in native script and original source of information/watch-list in Latin with the screening filter offering transliteration capability. For many markets, minimum standards are to screen the customer names against the media source names in Latin character sets.

Q13. What are the sources an FI might use for NNS?

Negative News can be found in a variety of publicly available media sources, with the screening being predominantly conducted through content published and accessed online. The credibility of the media source will be a key factor in determining whether it should be used in NNS. For example, factors such as the completeness, accuracy and coverage of the source should be considered.

Q14. How might an FI assess the credibility of Negative News Media Sources?

As part of a risk-based approach FIs should consider conducting an assessment on the sources used in NNS. Where an FI uses an external party or vendor to provide media sources or content, it is recommended that the FI understands the evaluation of reliability performed by the vendor and the controls they have in place to mitigate the risk of unreliable sources influencing the screening process.

In determining what constitutes a "good" source, the Group believes that typical characteristics of reputable sources are:

- Media Type: international news agencies and national newspapers which report on a broad spectrum of global and national events usually provide accurate and higher quality reporting. Regional and local news providers may report on events which are not covered by larger scale outlets, indicating that the reporting may only be deemed material to a specific location.
- Content: in larger scale primary media, credibility of the content is in general higher when subject to editorial oversight. There are a few factors which may indicate that a source is not reliable:
  - content is being corroborated from social media or appears to be non-professional
  - can be edited online by network participant(s), or
  - appears to be opinion-based[9].
- Geopolitical context: publications considered as politically neutral, or not fulfilling any specific political purpose would in general be more credible. Consideration should be given to news reported in countries with weaker democracies and/or non-democratic states where media may be controlled or influenced by leaders or leading parties. The presence of polarised news reporting should also be considered[10] and FIs should refer to sources such as the Press Freedom Index[11] to confirm the independence level of the press from political and corporate influence.
- Redundancy: in general, where the content of media sources can be substantiated by relevant or related material found in other reputable, the media sources are more reliable.
- Editorial Coherence: publishers who provide relevant details (e.g., statistics, dates, numbers, figures, names, and locations) and original source of information, cites, quotes or footnotes, usually represent higher quality and fact-based news. Sources where materials contain typographical, spelling, and other errors or lacking rhetorical structure may not be reliable. An author's linguistic choices and lexical diversity (e.g., emotional, extensive punctuation, eye-catching words) may indicate filtering of facts.
- Website Layout and Appearance: websites which appear to be poorly laid out or badly maintained may indicate less reliable content.

Q15. What is 'Disinformation'?

Disinformation (also known as 'Fake' or false news) is a global and multi-dimensional phenomenon which does not solely concern news media sources but has much broader societal and political reach. There is no universal term for disinformation, and in current use it has many possible, equally correct, naming conventions and determinations.

The risk that disinformation weakens the application of NNS may to some extent be mitigated through careful evaluation of sources such as the factors noted above under FAQ 14.

Q16. What Screening approaches might an FI use for NNS?

There are various tools available for FIs to manage effective NNS:

[9] For example, informal or personal content created by bloggers, vloggers, influencers.

[10] Media outlets from such jurisdictions varies greatly depending on political spectrum (e.g., right-wing, centralised, left-wing, conservative, nationalist, populist, liberal, socialist) and may report state-of-the-world in a partisan manner.

[11] Reporters Without Borders, *The World Press Freedom Index* ,https://rsf.org/en/world-press-freedom-index

- External: a solution provided by an external vendor/supplier. This covers technology, dataset and can include alert adjudication components outsourced to the vendor/supplier.
- Shared: only certain solution components[12] are provided by an external vendor/supplier. In this case, alert adjudication may be conducted internally or externally.
- Internal: a solution internally designed and deployed. This involves end-to-end NNS conducted internally, including data curation or screening against publicly available sources.

Q17. What factors might an FI consider when undertaking an evaluation of their NNS solution?

It is recommended that FIs conduct appropriate system evaluation to ensure that its screening solution is 'fit-for-purpose'. Assessments may include:

- Coverage: robustness of the data-base content and scope of monitored media sources. FIs should have sufficient media coverage in markets where the FI operates or where the customer base is located.
- Data: completeness, integrity, and timeliness of Negative News information. Consideration should be given to NNS accuracy and completeness, and levels of alert duplication if the same adverse data is found in multiple data sources.
- Matching: effectiveness of name matching, and false positive/alerts hit rate.
- Archive: accessibility of media articles which are archived or no longer available in open sources.
- Translation: capability to provide news/events translated into the language of the FI's operation.
- Scalability: ability to define search parameters, search depth and result filtering.
- Reporting: availability of relevant dashboards and performance metrics.
- Traceability: the recording and capability to review all internal screening events, configurations and other logic applied to generate a match.
- Data Sharing: consideration of local data-sharing requirements when utilising external/shared solutions, especially where external tools/teams are used to perform screening/adjudication on the FI's behalf.

Not all the above aspects can be assessed easily. For example, Internet-based NNS is limited and may hinder assessment of these criteria. Refer to FAQs 19-21 for further details.

Q18. Can an Internet Search Engine be used for NNS?

An Internet search engine is an on-line, algorithm-driven software designed to search information on the World Wide Web. Search engines are not databases but rather content browsing mechanisms. While Internet search engines may be used for certain aspects of NNS, it should be acknowledged that they have not been designed to assess Financial Crime Risk and may inadvertently de-prioritise information most relevant for this purpose. A reasonable effort should be made to understand the potential limitations associated with Internet-based screening prior to use.

Some Internet search engines allow a user to select specific search and results parameters[13]. More sophisticated engines provide advanced search options which can be used to specify terms, to position

[12] For example, dataset or technology.

[13] Including language and timeline of searches, number of results per page, or geographical span of searches.

content, file type and domain. However, it is recommended to maintain consistent settings to avoid inconsistencies in results or incorrectly applied search criteria.

It is also important to understand whether an Internet search engine enables both exact and partial matching. Depending on risk appetite, certain phrases should then be screened on an exact match basis to minimise the volume of irrelevant results[14], while other phrases may be searched on a partial match basis in order to maximise the opportunity to capture risk-relevant content[15]. FIs should consider the language in which screening is being conducted, as words written in local language may provide a different volume and quality of outcome than if the same words or phrases are searched in their translated version.

Q19. What is a Key Word in the context of NNS when using Internet Search Engines?

To achieve optimal results from Internet-based screening, it is recommended to define 'key words' (or 'key terms' or 'search phrases'), known as 'search strings' which will be screened along with an individual or entity name which is subject to NNS searches. There is no universally defined search string or globally agreed approach to defining Internet search key words, thus search string components and word order will vary across FIs. Search strings should be agreed internally and aligned to each FI's risk appetite, taking into consideration:

- Number of key words: the length of a search string should be reasonably shorter than the search engine word allowance. In circumstances where key words exceed the allowed number it may be appropriate to create supplemental search strings.
- Key words: An RBA should apply in deciding risk key words. Use of generic words, which refer to stages of a crime rather than crime itself, will affect the volume of alerts generated[16]. Therefore, it may be appropriate to select more precise terms when referring to type of the wrongdoing[17].
- Key words language: FIs need to determine the language in which searches will be conducted. The search string language may therefore depend on the jurisdiction where screening is conducted, customer location, or other relevant factors. Where FIs conduct multi language screening it is important to ensure that key words are translated correctly.

Q20. What are the limitations an FI should be aware of when using an Internet Search Engine for NNS?

Internet search engines, website owners or news purveyors have the right to purge, alter or archive the content at any time. Therefore, screening results may differ with each search, even if conducted using the same phrase or key words, depending on timing. FIs have no visibility nor oversight of Internet-based, publicly available content, therefore it cannot be easily determined whether the results presented are the most accurate, relevant, appropriate, or complete.

Content search, selection and results distribution, and the order in which they are presented, depend on numerous factors which are not visible or obvious to users. Internet Search Engines are algorithm-driven mechanisms which filter out content to match individual browsing preferences hence results can vary greatly across different users.

[14] For example, individual names, organisation names or two or multiple parts phrases such as 'tax evasion' or 'money laundering'.

[15] For example, 'bribe', 'corruption', 'smuggling', 'arrest'.

[16] For example: 'arrested', 'charges', 'investigation', 'alleged', 'probe', 'guilty'. Also, when selected terms can be used in broader context and are ubiquitous in nature, i.e., 'crime', 'misconduct' etc.

[17] Such as 'bribe', 'terrorism', fraud', 'theft' etc.

In many jurisdictions, the name of individuals or organisations subject to official criminal prosecution are not publicly available unless there are exceptional circumstances. Content can be subject to local, country-specific data protection regulation allowing removal of un-favourable information. In such scenarios using an Internet search engine for screening will be of limited value.

Q21 What factors should be considered when determining an operating model for NNS alert investigations?

Where NNS alerts are generated and meet the FI's criteria for investigation, it is important that a clearly defined end-to-end operating model and framework is in place to ensure the alerts are investigated and concluded in a timely and consistent manner.

To manage alert processing, an FI may choose to develop a tier-based investigation approach, e.g., an initial operational level undertaking high volumes of alert investigations against an agreed set of matching/discounting rules and procedures. Subsequent levels may be utilised where alerts cannot be discounted, or positive matches are identified, and due to the subjective nature of NNS outputs, require specialist subject matter expertise and input. This framework may differ between FIs, reflecting their size, scale, business activity and risk exposure.

Q22. What is meant by a Rules Based and Risk-Based approach to NNS Alert Management?

To support NNS alert investigations, an FI may develop a rules-based and/or a risk-based approach to alert investigations. A rules-based approach is a more prescriptive set of steps required to be completed to enable an alert investigation outcome to be determined. For example, NNS alerts are closed when the date of birth in the FI's customer record differs to the one published in the media by +/- 1 year. A risk-based approach enables the use of additional parameters and judgment, i.e., while elements of data match between the FI's customer and a NNS alert, other factors can be considered to determine the outcome such as the FI knows that the subject of Negative News is deceased, and the alert generation relates to live customer transactions.

Consideration should be given to the level of alert investigation needed and the knowledge and skills required by investigators.

Q23. Can Technology assist an FI in undertaking NNS?

There are a number of ways an FI can use technology to undertake NNS and manage alert volumes to ensure that investigations resources are focused on those alerts most likely to be productive, i.e., a 'positive' (or 'true') match /events for risk assessment. This may include the application of auto-discounting rules embedded within the screening tool, e.g., where irrelevant alerts are automatically discounted using pre-defined criteria.

Where technology is being used, it is important that FIs document all alert management solutions being used, the rationale for implementation and ensure that appropriate controls are in place to review periodically the performance of deployed applications.

Q24. What topics should be included in the procedures used by staff performing NNS?

Procedures should be in place for all steps in the process, be subject to a risk-based periodic review, and may include the following:

- Roles and Responsibilities: which outline the key roles in the end-to-end process and associated responsibilities.

- Assessment and Prioritisation of Alerts: which should be responsive to the risk screening prioritisation process, and if applicable, alert triage techniques. Furthermore, an FI's approach to handling a high volume of alerts in a risk-sensitive manner should be documented, e.g., via considering exact vs. partial matching, or other results narrowing criteria.
- Decision Making (Rules and Risk-Based Guidance): ensuring that alert adjudication is undertaken with a logical risk-based approach, with how to determine guidance on alert 'materiality'. For example, while a false positive alert would be discounted, a positive match could be considered 'material' where the nature of the information may indicate a heightened Financial Crime or Reputational Risk to the FI.
    - Discounting on the basis of a 'false positive' alert may include measures such as:
        - Where there is a significant difference between the customer's name and the name that is the subject of the news article.
        - Differences in key secondary identifier information (e.g., date of birth, date of incorporation, gender).
        - Consideration can be given toward other data points with "weaker" discounting criteria (e.g., profession, residence and other situational factors which make a positive match unlikely).
    - Discounting on the basis of 'immateriality' may include measures such as:
        - The FI's customer is not the subject (e.g., customer is a plaintiff).
        - Source of NNS is deemed not to be credible (e.g., blogs, tabloids).
        - Source is 'immaterial' in nature (e.g., does not relate to legal issues, regulatory issues or an issue that could present a risk to the FI or is reported by a source with questionable quality of information).
- Location of further internal/external customer information: providing guidance on supplemental, supporting information which may be used in an alert decisioning process.
- Referrals: instructions on what further investigation is to be conducted in cases where the outcome of NNS alerts investigation cannot be determined without further input from other departments and teams (e.g., the frontline/relationship manager teams).
- Recording of Outcomes and Rationale: providing requirements for a clear demonstration of the logic applied in alerts assessment and the rationale for decisioning made in respect of all alerts (including true and false positive matches) subject to review.
- Positive Match Escalation Approach: ensuring an appropriate escalation process for alerts deemed to be a positive match.
- Training: where an FI utilises specific IT equipment, systems or tools for alert investigation, documentation and training should be in place to ensure investigators understand how and why those systems and tools should be used.

Q25. What elements might be included in a training programme for staff performing NNS?

A comprehensive training programme for staff undertaking NNS investigations should consider the following elements:

- Financial Crime more broadly, the legal and regulatory environment and relevant policies and procedures.
- The alert investigation framework, including process, procedures, systems used, support available and escalation points.
- The importance of sound decision-making.
- Consequences of 'getting it wrong'.

- Empowering relevant staff to exercise critical thinking in the assessment of Negative News alerts.

Q26. What considerations should be given to Quality Control and Quality Assurance in the NNS Process?

Quality Control (QC) and Quality Assurance (QA) activities are key aspects in ensuring the effectiveness of the overall framework, control environment and mitigation of Financial Crime Risk.

QC is performed as a preventative control (pre-alert outcome determination), while QA is deemed a detective control (post-alert outcome determination). A strong control framework will contain elements of both.

An FI should ensure QC and QA processes are established to determine if alerts have been evaluated appropriately and risk managed in alignment with the FI's risk appetite.

Taking a risk-based approach, FIs should consider carrying out a risk assessment to determine the level of quality checks required and approach to the review, as well as the methodology used to extract an appropriate sample size and population for quality check or assessment (e.g., statistical vs. 'fixed' number). Where an FI can dedicate a proportionate degree of resources to quality check or quality assure selected alerts, a statistical based sampling should be viewed as the target approach.

Q27. Are there specific elements of Quality Assurance (QA) an FI should undertake?

To ensure effective and efficient NNS, FIs should evaluate and test the systems and processes used to evaluate quality and ensure applicable processes and systems are fit for purpose. A comprehensive QA programme will help identify vulnerabilities and process gaps to protect the FI from Financial Crime related risks:

<u>Systems</u>

- Assessment of the quality, accuracy and completeness of records returned from screening (e.g., all risk-relevant information and identifiers such as names, geographical reference, date of birth, gender are captured).
- Assessment of adequacy of system risk parameters and alert filtering mechanisms.
- Evaluation of the performance of the screening application by assessing the precision of screening and its hit rate.
- Oversight of the system input against returned matches to reconcile any missed screening records.

<u>Processes</u>

- Monitoring of the screening population to certify that the total number of alerts generated matches the total of alerts worked on (referred, dispositioned and/or closed). This gap analysis allows FIs to identify process gaps or missing alerts.
- Supervise the adherence to policies, procedures, and processes.
- Implement testing of NNS processed alerts to ensure compliance with agreed, risk-based discounting standards.
- Monitoring and testing of the false positive alert population to ensure there are no missed true matches.

Q28. What Key Management Information should be available for NNS?

Information should be made available to Management to provide regular reports on:

- The application effectiveness and efficiency criteria to measure the performance of NNS capabilities such as:
  - Screening volume
  - Volume of alerts generated
  - False positives and true matches
  - Quality assurance outcomes
- The relationships reviewed and exited by the FI due to NNS.

Q29. NNS is a broad topic, how would the Wolfsberg Group summarise NNS and the key areas to which an FI should give consideration?

NNS can be a valuable control in the management of Financial Crime Risk. There are many factors to consider in order for an FI to determine the appropriate level of NNS it should undertake. The implementation of NNS is part of the overall set of financial crime compliance controls and with the risk appetite of the FI at the centre of the approach taken. Given the potential scale of NNS, periodic effectiveness and efficiency testing will be essential to refining the approach taken by the FI to ensure NNS is optimised and adds value.

The Group believes FIs should seek to adopt a risk-based approach to NNS, specifically giving consideration to:

- The FI's overall financial crime compliance programme and control framework to identify Financial Crime Risk.
- The customers and business areas in scope of NNS, the risk categories and stages selected for screening.
- The challenges posed by disinformation and reliability of media sources and multi-language NNS.
- Selection of the most appropriate tools, e.g., third party suppliers, in house solutions and the use of Internet search engines.
- Technology being a key enabler in the effectiveness of identifying Financial Crime Risk through screening, more efficiently and on a real-time basis.
- The FI ensuring that people involved in the end-to-end NNS process are suitably trained, supervised, and that the appropriate levels of quality control and assurance are in place to ensure compliance with requirements.
- Robust management information should be made available to report effectiveness, efficiency, trends, and performance.

Glossary

Auto Discounting Rules: parameters which can be applied to alerts to discount them without the need for manual intervention. An example would be auto discounting any alerts where the customer's date of birth differs from the date of birth referenced in the media source by 1 year or more.

Batch Screening: an automated screening process eliminating manual input of individual or entity names Screening at periodic intervals provisioning alerts for review at a set time.

Keywords: the words of interest that will be screened e.g., 'money laundering' or 'bribe' to generate potential alerts and events of interest or for investigation.

Manual Screening: the screening of names input on an individual basis rather than in bulk.

Media Sources: the sources of information being used that contain the details of the risk events reported.

Risk and Event Stage: the stage (maturity) of the Negative News event, e.g., early stages of allegation or investigation, mid stage of a charge through to the final stage of conviction.

Risk Category: the category of interest for which keywords used in screening can be linked. This could often be the predicate offence, e.g., money laundering, human trafficking, terrorism.

Search Strings: often used in manual screening through internet search engines. The subject of interest is searched alongside selected keywords, e.g., John Smith plus 'money laundering', 'tax evasion'.

Structured Data: data that is specific, stored in a predefined format and can be easily accessed and used by a person or computer programme. An example would include a database entry of a negative news event tagged with the risk category and stage.

Transcription: is the process of transferring words written in one language script to another in accordance with a certain conversion system.

Transliteration: the process of transferring a word from the alphabet of one language to another to aid pronunciation. Transliteration changes the letters from the words original alphabet to similar sounding letters in a different alphabet.

Unstructured Data: unfiltered raw data that when searched, will typically return broad results. An example would include sources from social media.