aml

From: [redacted]@hsbc.co.nz>
Sent: Friday, 3 December 2021 4:41 pm
To: aml
Cc: [redacted]
Subject: HSBC NZ submission - AML/CFT Act consultation feedback
Attachments: Consultation feedback-HSBC.pdf

Hi AML/CFT Act consultation team

Please find attached HSBC New Zealand's submission on changes to the AML/CFT Act.

If you need further information, please let us know.

Kind regards
[redacted]

[redacted]
Country Head – Oversight & Reporting | Compliance
The Hongkong and Shanghai Banking Corporation Limited
HSBC Tower, Level 21, 188 Quay Street, Auckland 1010

Telephone: [redacted]
Mobile: [redacted]
E-mail: [redacted]@hsbc.co.nz

AML/CFT Statutory Review Consultation Feedback

Date: 3 December 2021

Prepared by: The Hongkong and Shanghai Banking Corporation Limited (HSBC), New Zealand

HSBC

Table of Contents

Summary

HSBC is pleased to respond to the Ministry of Justice's (MOJ) consultation on the AML/CFT Act. HSBC is represented through the New Zealand Bankers Association response, however, would also like to provide some further thoughts for consideration.

HSBC supports the Government's ambition for a more effective framework to manage financial crime risk and welcomes the constructive engagement on the future regulatory framework. The review of the AML/CFT Act is important if New Zealand (NZ) is to be as effective as possible in detecting and deterring illicit activity now and in the future. It is recommended that this work should be incorporated as part of a wider review of the regulatory framework related to economic crime, including reforms to the Companies Office.

HSBC has identified a number of areas which it wishes to highlight in response to the review. As a starting point, we stress that for an AML/CFT framework to be effective, it must have a shared outcomes-focused high-level objective, with the public and private sectors working to protect the financial system and broader economy from money laundering and terrorist financing. An emphasis on the desired outcome and away from process would redeploy supervisory efforts from focusing primarily on technical compliance and allow reporting entities to focus resource on tackling high risk activity. Adopting a more risk-based approach to managing financial crime risk is critical in this regard, particularly when it comes to the use and adoption of transformative technologies.

HSBC also strongly encourages greater collaboration and information sharing between public and private sectors. Having access to the right information is central to tackling illicit finance. More and more information is held by the private sector, and there are enhanced intelligence capabilities within banks and other reporting entities. But there are barriers to sharing information between the private sector and governments, and within the private sector, including within banking groups. The ability to share information within a defined framework will enable the public and private sectors and private sectors to deepen cooperation to ensure our efforts are targeted in the right places. HSBC would encourage the government to prioritise legislation that will enable greater information sharing for the purposes of tackling economic crime.

HSBC would be happy to discuss any of the points raised in this response.

Purpose of the AML/CFT Act

1.1. Are the purposes of the Act still appropriate for New Zealand's AML/CFT regime or should they be changed? Are there any other purposes that should be included other than what is mentioned?
HSBC considers that the current purposes of the Act remain appropriate.

1.2. Should a purpose of the Act be that it seeks to actively prevent money laundering and terrorism financing, rather than simply deterring or detecting it?
HSBC believe that including prevention as a purpose of the act imposes unreasonable burden on the reporting entities and may have undesirable effects or unintended consequences on the reporting entities' management of financial crime risks.

1.3. If so, do you have any suggestions how this purpose should be reflected in the Act, including whether there need to be any additional or updated obligations for businesses?
A preventative purpose would work best if primarily directed at enhancing tools for law enforcement, rather than revising obligations for reporting entities.

Understanding our risks

1.7. What could be improved about New Zealand's framework for sharing information to manage risks?

Feedback from law enforcement

HSBC would welcome more direct and regular feedback from the FIU on intelligence provided to them. This would help banks to further enhance their internal monitoring capabilities to detect illicit activity.

Feedback from supervisors

HSBC would welcome more direct and regular feedback from supervisors regarding best practice identified from onsite inspections.[1]

Information Sharing

Data privacy laws and the inconsistent application of legal gateways for information-sharing remain a barrier to an effective regulatory and supervisory regime. HSBC would encourage the government to prioritise legislation that will enable greater information sharing for the purposes of tackling economic crime. HSBC would recommend the MOJ engage with Monetary Authority of Singapore on the work currently being undertaken on such a framework.

1.8. Are the requirements in section 58 still appropriate? How could the government provide risk information to businesses so that it is more relevant and easily understood?

There is scope for the Act to be less prescriptive in terms of the areas covered under section 58. E.g. there is considerable overlap between the categories and often leads to repetitive information being provided in the risk assessment to meet auditor expectations. The information contained in the category of nature, size and complexity is often duplicated in the other categories. Additionally, for larger reporting entities using more sophisticated risk tools, it becomes harder to segregate the risk assessment into pre-defined categories. Using an example of banks, it is difficult to distinguish between internet banking as a product or service and international banking as a country risk, product risk or service risk. This is one area where perhaps a risk-based approach that is less prescriptive would work better, particularly as the Act has been in force for almost a decade and reporting entities are better equipped to describe and assess their risks.

Balancing prescription with risk-based obligations

1.9. What is the right balance between prescriptive regulation compared with the risk-based approach? Does the Act currently achieve that balance, or is more (or less) prescription required?

It would be useful for the Act to be either fully risk-based or more prescriptive because a combination of the two causes ambiguity and differences of opinion between supervisors. An example is the risk rating of trusts where the Reserve Bank of New Zealand (RBNZ) require trusts to be rated high risk but this is not a requirement by other supervisors. RBNZ reporting entities are unable to take a risk-based approach while other reporting entities are able to. It is not clear why the same customer type is considered high risk by one supervisor but not by others. This leads to customer confusion as the same customer may have fewer risk-based measures applied to them under the same piece of legislation by a different reporting entity. HSBC's preferred approach would be for a more risk-based approach to be adopted.

1.10. Do some obligations require the government to set minimum standards? How could this be done? What role should guidance play in providing further clarity?

Guidance is beneficial in terms of providing more information on how to comply with certain sections of the Act or regulations that are complex or ambiguous. It would be useful for the government to define standards around new or developing technologies/products that favour anonymity as this

1 Source: New Zealand Bankers Association draft submission 211118

obligation is interpreted differently by reporting entities. E.g. some entities may consider digital currencies established rather than new/developing while others may not.

1.11. Could more be done to ensure that businesses' obligations are in proportion to the risks they are exposed to?
Yes, the Act could be less prescriptive and allow reporting entities to take a more risk-based approach to compliance. However, this could potentially cause issues in terms of supervision if supervisors need to determine if the approach followed is really 'risk-based' or based on the 'least stringent measures'. It may require closer or more frequent supervision.

Applying for exemptions from the Act

1.14. Are exemptions still required for the regime to operate effectively? If not, how can we ensure AML/CFT obligations are appropriate for low-risk businesses or activities?
Yes, they are still appropriate as reporting entities may require exemptions from specific sections of the Act rather than an exemption from the Act altogether. There could be valid reasons for exemption requests e.g. difficulty complying with a prescriptive obligation; however, able to meet the spirit or risk-based requirement of the obligation.

1.15. Is the Minister of Justice the appropriate decision maker for exemptions under section 157, or should it be an operational decision maker such as the Secretary of Justice? Why or why not?
An operational decision maker would be more suitable to speed up the process of exemption review and approval. HSBC would be supportive of the supervisors having the authority to decide on exemptions.

1.16. Are the factors set out in section 157(3) appropriate?
Yes, it is appropriate to list out minimum criteria for assessing an application to ensure a fair and consistent review of exemption requests.

1.17. Should it be specified that exemptions can only be granted in instances of proven low risk? Should this be the risk of the exemption, or the risk of the business?
No, there may be instances where the risk is mitigated by other measures and proof of low risk may be difficult to establish.

1.18. Should the Act specify what applicants for exemptions under section 157 should provide? Should there be a simplified process when applying to renew an existing exemption?
Yes, it would be helpful if the Act could define minimum requirements that must be provided for exemptions. Similarly, a simplified process, either reconfirming previous submissions or providing up-to-date data/risk assessments would work for renewing exemptions.

1.20. Are there any other improvements that we could make to the exemptions function? For example, should the process be more formalised with a linear documentary application process?
Yes, either a standard application template or a list of mandatory requirements would make the process easier to manage.

Mitigating unintended consequences

1.21. Can the AML/CFT regime do more to mitigate its potential unintended consequences? If so, what could be done?
1.22. How could the regime better protect the need for people to access banking services to properly participate in society?

1.23. Are there any other unintended consequences of the regime? If so, what are they and how could we resolve them?

Address verification

Address verification requirements currently disadvantage vulnerable customers, customers who do not have a residential address or move accommodation regularly.

Customer exit management

Current requirements around the management of customer exits create potentially challenging circumstances for reporting entities. For example, if a customer does not provide Know Your Customer (KYC) information for Enhanced Customer Due Diligence (ECDD), reporting entities must exit the relationship. This could result in a reporting entity having to unwind existing contracts prematurely e.g. forcing a customer to repay their mortgage (and potentially default on their mortgage if unable to refinance) simply because we could not contact the customer would not be a good conduct outcome for the customer. HSBC believe there are other tools to effectively manage and mitigate the risk without having to terminate existing business relationships.

Designated Business Groups (DBG)

Please refer to the responses under question 3.9.

Data Privacy & Information Sharing

Data privacy and information sharing frameworks significantly restrict the ability of reporting entities to conduct value-add investigations. Addressing this could significantly enhance the investigation capability of reporting entities, reduce the burden on law enforcement and help reporting entities make more informed, risk-based decisions on the customers they maintain.

Identity verification can pose challenges

The Amended Identity Verification Code of Practice (IVCOP) is restrictive for customers who are unable to obtain a passport or driver's licence. Banks use their exemption handling processes where appropriate, however, we note this can lead to delays in account opening and can create frustration for customers. Increasing the available primary and secondary identification options within IVCOP should reduce reliance on exemption provisions[2].

Partnering in the fight against financial crime

1.24. Can the Act do more to enable private sector collaboration and coordination, and if so, what?

1.25. What do you see as the ideal future for public and private sector cooperation? Are there any barriers that prevent that future from being realised and if so, what are they?

1.26. Should there be greater sharing of information from agencies to the private sector? Would this enhance the operation of the regime?

Having access to the right information is central to tackling illicit finance. Collectively, we need to make the system for managing financial crime risk more effective, and we need to look at how we can make it more risk-based. More and more information is held by the private sector, and there are enhanced intelligence capabilities within banks and other reporting entities. But there are barriers to sharing information between the private sector and governments, and within the private sector, including within banking groups. Barriers exist in most jurisdictions and include: different regional and jurisdictional data protection laws, bank secrecy laws, customer confidentiality requirements, outsourcing, and 'tipping-off' concerns.

Intelligence provided by the public sector can provide information on specific entities, but often lacks key details on, for example, individual transactions. By contrast, banks see end-to-end global payment

2 Source: New Zealand Bankers Association draft submission 211118

flows, but lack specific indicators of which payments are tied to criminality, relying instead on a system of filters and electronic monitoring to spot anomalies. We need to deepen cooperation between the public and private sectors and within the private sector (including within banking groups) to ensure our efforts are targeted in the right places.

Data privacy laws and the inconsistent application of legal gateways for information-sharing remain a barrier to an effective regulatory and supervisory regime. HSBC would encourage the government to prioritise legislation that will enable greater information sharing for the purposes of tackling economic crime. HSBC would recommend the MOJ engage with Monetary Authority of Singapore on the work currently being undertaken on such a framework.

Allowing information to be requested from other businesses

1.28. Should the FIU be able to request information from businesses which are not reporting entities in certain circumstances (e.g. requesting information from travel agents or airlines relevant to analysing terrorism financing)? Why or why not?
1.29. If the FIU had this power, under what circumstances should it be able to be used? Should there be any constraints on using the power?
1.30. Should the FIU be able to request information from businesses on an ongoing basis? Why or why not?
1.31. If the FIU had this power, what constraints are necessary to ensure that privacy and human rights are adequately protected?
HSBC is supportive of the FIU to have the ability to request data that allows it to form a full picture of a scenario but the purpose of the information request should be clear and usage of the data should be restricted to the purpose identified. Data obtained through the process should not be shared with other government agencies to prevent privacy and human rights violations.

Freezing or stopping transactions to prevent harm

1.32. Should the Act provide the FIU with a power to freeze, on a time limited basis, funds or transactions in order to prevent harm and victimisation? If so, how could the power work and operate? In what circumstances could the power be used, and how could we ensure it is a proportionate and reasonable power?
HSBC is supportive of the FIU having a power to freeze funds or transactions in instances where Police become aware of proceeds of crime and require time to complete an initial investigation and obtain a Court Order to restrain the funds[3].

1.33. How can we avoid potentially tipping off suspected criminals when the power is used?
There is no way to freeze an account without a customer knowing. If the Police intend to freeze funds, they should be prepared to engage directly with the individual/entity impacted. The reporting entities' role should be limited to freezing the account, with Police handling all communications.[4]

Codes of Practice

1.39. Should the New Zealand Police also be able to issue Codes of Practice for some types of FIU issued guidance? If so, what should the process be?
Yes, the FIU should be able to issue codes of practice in relation to SARs, PTRs, transaction monitoring, etc. There should be a consultation process with reporting entities to understand the impact to smaller and/or multi-jurisdictional entities as they may be impacted disproportionately.

3 Source: New Zealand Bankers Association draft submission 211118

4 Source: New Zealand Bankers Association draft submission 211118

1.40. Are Codes of Practice a useful tool for businesses? If so, are there any additional topics that Codes of Practice should focus on? What enhancements could be made to Codes of Practice?
Yes, some elements of the codes of practice are useful; however, some are too prescriptive for multi-jurisdictional reporting entities. It is important that they are consistently interpreted across the three supervisory authorities in their application.

1.41. Does the requirement for businesses to demonstrate they are complying through some equally effective means impact the ability for businesses to opt out of a Code of Practice?
Yes - reporting entities are hesitant to opt out of a code of practice as it is difficult to determine what would qualify as 'equally effective means'. Additionally, the risk of being assessed as partially compliant when opting out of a code of practice means that reporting entities are less likely to opt out.

1.42. What status should be applied to explanatory notes to Codes of Practice? Are these a reasonable and useful tool?
Clarity is needed on the legal position of explanatory notes. It is unclear whether they hold the same status as codes of practice or merely clarify the codes of practice. It would be beneficial if the code of practice itself contained more details and the explanatory note was not needed.

Non-profit organisations vulnerable to terrorism financing

2.37. Should tax-exempt non-profits and non-resident tax charities be included within the scope of the AML/CFT Act given their vulnerabilities to being misused for terrorism financing?
HSBC is supportive of tax-exempt non-profits and non-resident tax charities to be included within the scope of the Act.

1.38. If these non-profit organisations were included, what should their obligations be?
Similar to registered charities e.g. requirements to list key controllers, purpose/beneficiaries, minimum requirements for audited financials.

Agency supervision model

3.1. Is the AML/CFT supervisory model fit-for-purpose or should we consider changing it?
3.2. If it were to change, what supervisory model do you think would be more effective in a New Zealand context?
3.3. Do you think the Act appropriately ensures consistency in the application of the law between the three supervisors? If not, how could inconsistencies in the application of obligations be minimised?
3.4. Does the Act achieve the appropriate balance between ensuring consistency and allowing supervisors to be responsive to sectoral needs? If not, what mechanisms could be included in legislation to achieve a more appropriate balance?
It would be preferable to have a single supervisor/regulator to avoid inconsistencies between supervisors and provide greater clarity to the market on AML/CFT requirements (both reporting entities subject to the Act and the customers of the reporting entities). The current model with different supervisors having different approaches to the same piece of legislation/guidance is confusing. This can also create complexities to issue joint publications e.g. delays in gathering/publishing information.

HSBC is supportive of a risk-based supervision model.

Powers and functions

3.5. Are the statutory functions and powers of the supervisors appropriate or do they need amending? If so, why?

It would be useful if the supervisors had greater powers in terms of exemption/temporary exemption requests and more enforcement powers.

Remote inspections

3.7. What are some advantages or disadvantages of remote onsite inspections?

3.8. Would virtual inspection options make supervision more efficient? What mechanisms would be required to make virtual inspections work?

The advantage of virtual inspections is that they can be done even if the supervisor/reporting entity is based in a different city or if there are travel restrictions. It is likely to be cheaper and reduce the environmental impact. The disadvantages are that it is likely to require more effort to coordinate a virtual inspection as data will need to be extracted from systems (sometimes taking weeks), technological constraints for virtual meetings. This could increase the duration of inspections.

Designated Business Groups

3.9. Is the process for forming a DBG appropriate? Are there any changes that could make the process more efficient?

The current requirements to form a designated business group do not cater for global organisations. HSBC New Zealand is currently restricted from sharing information with other members of the HSBC Group or benefitting from other benefits provided for a DBG despite the fact that many of our customers bank with us across multiple jurisdictions and many services are provided centrally. It is not feasible for us to form a DBG with other HSBC Group entities due to the size, nature, number and complexity of the HSBC Group. HSBC acknowledges that certain restrictions afforded by the current DBG model can be addressed through other sections of the act e.g. agency agreements or information-sharing relating to SARs. HSBC recommends the MOJ adopt the measures outlined in the interpretive note to FATF Recommendation 18 (financial institution group-wide information sharing).

Independent auditors

3.11. Should explicit standards for audits and auditors be introduced? If so, what should those standards be and how could they be used to ensure audits are of higher quality?

Yes, it would be beneficial to list what elements of a risk assessment or programme must be covered and to what extent i.e. the depth and scope of the audit. It would also be useful to specify the minimum requirements for someone to qualify as an auditor e.g. technical skills in risk/audit/compliance. It would not be sufficient to list audit qualifications as financial auditors do not always have the necessary knowledge of the Act to be able to conduct these types of audits.

3.12. Who would be responsible for enforcing the standards of auditors?

The supervisors. If the model of three separate supervisors continues, an audit firm/auditor auditing a particular type of reporting entity could be supervised by the same supervisor as the reporting entity.

3.13. What impact would that have on cost for audits? What benefits would there be for businesses if we ensured higher quality audits?

It would increase the price of audits as it would mean that the audits are more than a checklist of activities and there is adequate testing that is undertaken. It would probably impact smaller reporting entities disproportionately as the larger entities would most likely use internal audit teams or be able to easily secure the services of one of the large audit firms.

The benefits would be an opportunity to:

- identify deeper issues with compliance rather than documentation-related observations around how a risk assessment/programme is written
- benchmark themselves against other reporting entities due to a consistent standard
- undertake industry-wide action where needed
- implement more realistic/pragmatic solutions, in line with the size of the business/customer base

3.14. Should there be any protections for businesses which rely on audits, or liability for auditors who do not provide a satisfactory audit?
Yes, there should be both protections and liabilities. If there is a consistent standard for auditors and audits, it would be reasonable for businesses to rely on them to identify (within reasonable limits) any gaps in compliance. It would also put the onus on auditors' testing methodologies to ensure that it adequately captured the risk of the business and was not merely a checklist audit or an attestation from the entity being audited.

Consultants

3.15. Is it appropriate to specify the role of a consultant in legislation, including what obligations they should have? If so, what are appropriate obligations for consultants?
HSBC does not consider it appropriate to specify the role of a consultant in legislation.

Agents

3.18. Do you currently use agents to assist with your AML/CFT compliance obligations? If so, what do you use agents for?
Yes. Agents are currently used for the purposes of Customer Due Diligence (CDD).

3.19. Do you currently take any steps to ensure that only appropriate persons are able to act as your agent? What are those steps and why do you take them?
Yes, they must be either part of the group company or a New Zealand AML/CFT reporting entity to ensure that they have a minimum standard of AML/CFT compliance requirements, including record-keeping and privacy.

3.20. Should there be any additional measures in place to regulate the use of agents and third parties? For example, should we set out who can be an agent and in what circumstances they can be relied upon?
It would be useful to specify minimum standards for agents/third parties that are relied on e.g. criteria they must meet, the information the agent must provide at a minimum, the time period within which they must respond to reporting entities' requests for information, etc.

Allowing for intermediary enforcement options

3.21. Does the existing penalty framework in the AML/CFT Act allow for effective, proportionate, and dissuasive sanctions to be applied in all circumstances, including for larger entities? Why or why not?
No - the Act has been in force for almost a decade and actions to ensure compliance should be stronger as reporting entities have had sufficient time to prepare for this. Some supervisors like the Department of Internal Affairs (DIA) have taken stronger action against smaller entities while action against larger entities has been slower, potentially due to the size of the entities and the impact any enforcement action will have on the economy/industry. A penalty framework should be fair, transparent, proportionate and risk-based. The penalty regime should deter non-compliance and take into consideration positive behaviour where appropriate.[5]

5 Source: New Zealand Bankers Association draft submission 211118

3.22. Would additional enforcement interventions, such as fines for non-compliance or enabling the restriction, suspension, or removal of a licence or registration enable more proportionate, effective, and responsive enforcement?
Yes, however, it is important that reporting entities are able to assess regulatory risk exposure as accurately and clearly as possible.[6]

Sanctions for employees, directors, and senior management

3.25. Would broadening the scope of civil sanctions to include directors and senior management support compliance outcomes? Should this include other employees?
Yes – it would ensure that there is more personal responsibility for decisions made. It should include compliance officers who make decisions for the firm.

3.27. Should compliance officers also be subject to sanctions or provided protection from sanctions when acting in good faith?
Yes – it would ensure that when a compliance officer is being appointed to the role, there is sufficient consideration as to the appropriateness of the candidate and their ability to make sound, ethical decisions. There should be provisions to provide protection to compliance officers when they are acting in good faith e.g. recommended a particular course of action which was disregarded by senior management.

Customer due diligence

4.1. What challenges do you have with complying with your CDD obligations? How could these challenges be resolved?
Collection and verification of address.
Address verification does not work particularly well and it is unclear what the purpose of address verification is. If it is to keep a record of customers' primary residence for Suspicious Activity Reports (SAR)/law enforcement purposes, most customers move often and as they do not receive physical mail from the reporting entity, they do not update their address details when they move. Additionally, address verification is increasingly not being used internationally and is difficult to obtain from international customers who raise both privacy and legislative concerns for cross-border transfer of data. If the Act could remove the requirement to verify a customer's address, it would be beneficial both in terms of cost of compliance and customer experience.

Identification and verification
The IVCOP identity document options could be simplified, particularly with respect to overseas driver's licences e.g. the requirement to hold an international driver's permit could be removed, instead relying on an overseas driver's licence as a photographic form of identity and other forms of non-photographic identity.

Customers often provide recently expired identity verification. Reporting entities should be able to take a risk-based approach toward accepting recently expired identity verification.

Certification
There are inconsistencies in the certification rules in New Zealand and overseas, so we sometimes see overseas customers provide documentation that is legitimately certified in their country but not in New Zealand.[7]

6 Source: New Zealand Bankers Association draft submission 211118

7 Source: New Zealand Bankers Association draft submission 211118

In addition, the 3-month certification validity period should be removed provided the identity is still valid, as often customers hold previously certified documents.[8]

'Wet ink' Certification

The obligation to obtain 'wet ink' certification on identification documents is no longer fit for purpose given technological developments e.g. digital signatures/certification could be permitted. It would also be beneficial to include details of any digital certification in the code of practice to allow reporting entities to be more consistent in their approach towards customers.

Politically Exposed Persons (PEPs)

The PEP definition for entity customers covers beneficial ownership of more than 25% which is similar to other customer types. However, this is challenging when dealing with state-owned entities in overseas jurisdictions as in certain countries, almost all entities are state-owned. HSBC would recommend adopting a risk-based approach to allow a different threshold e.g. 50% (or higher) owned by the state and a significant influence trigger (e.g. ability to control/influence senior management appointments) when dealing with entity customers who are owned by the state.

Ultimate Beneficial Ownership (UBO)

A global network of national UBO registers would be a significant enhancement of the global AML/CFT arrangements and would be one of the most powerful weapons against abuse of the financial system for a wide range of crimes including money laundering, bribery and corruption, tax evasion, fraud and terrorist finance. The key components of a global network would be accurate, up-to-date, verified and accessible national UBO registers that enable public and private sector entities to identify, report and mitigate financial crime risk arising from abuses of the legal person in their jurisdiction, as defined by national laws. National registers can serve as a focal point for improving collective understanding of local risks and for public-private partnerships to reduce exploitation of the financial system.

There are three main problems with the current arrangements for UBO registration (NB: these are generic observations of UBO registries worldwide and not specific to NZ Companies Office):

- Inaccuracy: While UBO registers already exist in a number of jurisdictions, most carry large amounts of inaccurate information. These inaccuracies arise from errors or omissions companies may commit in the original filings, stale information resulting from failures to register changes or to complete mandatory updates to those original filings, and deliberate attempts to mislead authorities in order to avoid tax or to conceal other criminal activity. As a result, public and private sector consumers of the information held in the UBO register cannot rely upon it, or use it to improve their management of risk.
- Lack of Verification: The inaccuracies described above remain uncorrected because, in the case of most existing UBO registers, information is not subject to rigorous independent verification by the register authority. Many authorities lack access to reliable sources of data, including that held by other departments of their own government, with which to cross-reference the filings. Few are applying the advanced technology and analytical techniques that could enhance the verification process. (NB: Recent work of the World Economic Forum, Financial Action Task Force and the B20 can provide valuable context.)
- Accessibility: UBO registers in some jurisdictions are not fully accessible to private sector entities seeking to manage financial crime risk. Restriction of relevant information, whether

8 Source: New Zealand Bankers Association draft submission 211118

by design (e.g. due to data privacy concerns) or as a result of slow or inconsistent administration, leads to missed opportunities to improve collective knowledge and raise the integrity of the overall regime.

HSBC's view is that:

1. Companies (and Trusts) have the best understanding of their own UBO structures. We are strongly in favour of properly enforced legal requirements for companies to self-certify their UBO structure when filing to the register. Registers will need to remain up-to-date. Changes in the ownership and control structure should be reflected promptly in the register, with a short statutory notification period in which filing entities must record changes to their UBO structure (and sanctions for failure to do so). Shareholders should be under a similar requirement to inform companies of changes that could affect the UBO structure of the company.
2. Register authorities should have access to a broad range of government-held information, including formally from the private sector (e.g. through SARs, FATCA, CRS) and should be able to exploit data from trustworthy sources (e.g. telecom providers) and open source media. Discrepancy reporting from obliged entities should provide a check and balance to information stored on the register, but cannot make up for failures to enforce accurate filings to the register, or for poor verification of these filings by register authorities. Register authorities should seek continuous improvement in terms of technical design, data management and cyber security, analytical methodology and resourcing.
3. Provisions must be made to give banks and other private sector bodies access to information held in UBO registries. Automatic access, i.e. such that changes in the register are automatically notified to reporting entities, would further reduce risks arising from discrepancies between the register and private sector records. All access to UBO register information must be proportional from a data privacy perspective in order to retain the confidence of the public (our customers).
4. In order to facilitate interoperability of national registers worldwide, clear definitions of key terms and data harmonisation will be essential.

Beneficial Ownership of Trusts

Determining the beneficial owners of a trust is a concern, particularly in the case of beneficiaries with a vested interest of more than 25% in the trust property. There is confusion about the definition of 'vested interest' with some reporting entities interpreting this as the time the benefit is realised (i.e. trust benefits being paid out) and some interpreting it as a potential benefit (i.e. benefit that will be realised at some stage in the future). There is additional confusion around how this needs to be interpreted in the context of a discretionary trust where the trustees can change beneficiaries at any point. This leads to inconsistent approaches to compliance. There is an element of cost involved with getting it right and it would be useful if the supervisors could clarify the position in this respect. It should be noted that in some jurisdictions, for unnamed beneficiaries, identification and verification is only required on payment of benefits not at the outset.

Risk treatment of trusts

RBNZ require trusts to be rated high risk but this is not a requirement by other supervisors. RBNZ reporting entities are unable to take a risk-based approach while other reporting entities are able to. It is not clear why the same customer type is considered high risk by one supervisor but not by others. This leads to customer confusion as the same customer may have fewer risk-based measures applied to them under the same piece of legislation by a different reporting entity. HSBC recommends a more risk-based approach to be adopted to determine the appropriate level of CDD conducted on trusts.

Digital Identity (ID)

The capability for digital identification and verification is a defining element of an effective AML/CFT regime. A solution is for reporting entities to obtain secure digital access to a wide range of customer data attributes from reputable sources, always predicated on customer consent. This must include on-demand digital access to:

- Government-held sources such as passport issuing agencies, beneficial ownership registers, records on citizens' employers
- Customer data from public and private utility companies (energy, telecommunications etc.), large scale online merchants.

Digital access to a wide range of customer data attributes from reputable sources will allow us to:

1. Review a greater range of data more regularly, triggered where appropriate by changes in the data, and without asking customers to present to us in a physical format.
2. Conduct CDD and ECDD processes that are more risk-focused, reducing the impact on innocent customers.
3. Improve financial inclusion by seeking out data assurance for KYC for customers who might otherwise be excluded as a result of not possessing traditional (paper) documentation such as a passport or utility bill.
4. Keep pace with fast evolving financial crime threats by giving us the opportunity to request additional digital data attributes as they become available.

Direct access to identity attributes enables a clear and proportionate resolution of the question of liability, as each consuming institution will make its own decision on the basis of the attributes it deems important and how they choose to use those attributes. Regulators/supervisors will need to be able to assess each institution's approach to risk and their use of data to mitigate it.

Relationship to the customer

The requirement to verify the relationship to the customer is unclear and causes confusion. It would be useful to specify either through guidance or a code of practice what is required to verify a person's relationship to a customer. There are limited documents independent of the customer to verify this element of CDD. E.g. if an entity customer's finance manager acts on their behalf to transact on the account, the verification would be either a letter from the customer or their employment ID both of which are not independent of the customer.

Dormant customers

There is insufficient clarity around dormant or inactive customers who were on-boarded prior to the commencement of the Act. If these customers cannot be contacted or do not respond and funds are unable to be returned, their business relationship cannot be terminated nor can CDD be completed. It would be useful if guidance could be provided in terms of regulatory expectations for these customers.

When CDD must be conducted

4.10. For enhanced CDD, is the trigger for unusual or complex transactions sufficiently clear?
4.11. Should CDD be required in all instances where suspicions arise?
4.12. If so, what level of CDD should be required, and what should be the requirements regarding verification? Is there any information that businesses should not need to obtain or verify?

Yes the trigger is sufficiently clear. However, the requirement to complete ECDD on submission of a SAR should be reviewed due to the potential for tipping off a customer. In addition, exceptions should be made to this requirement if a reporting entity determines that the suspicious activity is not within appetite and a decision to terminate the business relationship is made.

What information needs to be obtained and verified

1.18. Is the information that the Act requires to be obtained and verified still appropriate? If not, what should be changed?
4.19. Are the obligations to obtain and verify information clear?
4.20. Is the information that businesses should obtain and verify about their customers still appropriate?
Please refer to responses under question 4.1.

The 'person on whose behalf a transaction is conducted'

4.35. Should we issue a regulation which states that for the purposes of the definition of beneficial owner, a person on whose behalf a transaction is conducted is restricted to a person with indirect ownership or control of the customer (to align with the FATF standards)? Why or why not?
Yes, this would be very beneficial. This could apply in situations where power of attorney has been assigned. Currently, this is unclear, leading to reporting entities verifying the identity of persons who may not have ownership or control of the customer.

4.36. Would this change make the "specified managing intermediaries" exemption or Regulation 24 of the AML/CFT (Exemption) Regulations 2011 unnecessary? If so, should the exemptions be revoked?
Yes, it would to a large extent. If the issue about control of the customer is addressed adequately in the Act, the exemptions about underlying customers would not be needed. However, the exemptions pertaining to LMI/SMI beneficial ownership may still be useful.

4.42. Should we issue regulations or a Code of Practice that allows businesses to satisfy their beneficial ownership obligations by identifying the settlor, the trustee(s), the protector and any other person exercising ultimate effective control over the trust or legal arrangement?
It would be useful to provide a code of practice or regulations to clarify the beneficial ownership requirements for beneficiaries of trusts, particularly as they often do not control the trust assets and in some instances, may not even be aware that they are beneficiaries of a trust. In instances where beneficiaries are also trustees or have control of the trust's assets, it would be prudent to clarify that effective controller requirements apply.

Identity Verification Code of Practice

4.45. Do you encounter any challenges with using IVCOP? If so, what are they, and how could they be resolved?
4.47. Should we amend or expand the IVCOP to include other AML/CFT verification requirements, e.g. verifying name and date of birth of high-risk customers verifying legal persons or arrangements, ongoing CDD, or sharing CDD information between businesses?
4.48. Are there any identity documents or other forms of identity verification that businesses should be able to use to verify a customer's identity?
It would be beneficial to clarify whether documents can be certified virtually. E.g. during the pandemic, changes were made to the Oaths & Declaration Act to allow for virtual declarations; however, this did not apply to certifications, sometimes causing confusion for customers who did not understand the difference between the two processes.

It would be useful to clarify requirements for higher risk customers and ongoing CDD as these are areas where there is inconsistency between reporting entities.

Please also refer to the responses under question 4.1.

Verifying the address of customers who are natural persons

4.50. What challenges have you faced with verification of address information? What have been the impacts of those challenges?
4.51. In your view, when should address information be verified, and should that verification occur?
4.52. How could we address challenges with address verification while also ensuring law enforcement outcomes are not undermined? Are there any fixes we could make in the short term?
Please refer to responses under question 4.1.

Mandatory enhanced CDD for all trusts

4.58. Should we remove the requirement for enhanced CDD to be conducted for all trusts or vehicles for holding personal assets? Why or why not?
4.59. If we removed this requirement, what further guidance would need to be provided to enable businesses to appropriately identify high risks trusts and conduct enhanced CDD?
4.60. Should high-risk categories of trusts which require enhanced CDD be identified in regulation or legislation? If so, what sorts of trusts would fall into this category?
Yes, HSBC supports a risk-based approach to determining the appropriate level of CDD applied to trusts. All trusts are not inherently high risk and there are many small family trusts with the only asset being the family home. These customer types are often lower risk than companies with complex structures yet are treated in a similar manner.

The guidance could include specific risk factors that make particular types of trusts high risk e.g. type of trust, country of establishment, country of tax residency, entities that exercise control over the trust, etc. We would recommend the supervisors provide guidance on indictors that may present a higher risk of illicit activity that warrant ECDD.

Ongoing customer due diligence and account monitoring

4.61. Are the ongoing CDD and account monitoring obligations in section 31 clear and appropriate, or are there changes we should consider making?
It would be useful to clarify whether updated identification documents must be verified and whether expired identity documentation needs to be refreshed as part of OCDD.

Greater clarity could be provided on what information must be checked and updated during an ongoing CDD review and whether certain information can be inferred from transactional activity.[9]

It would be useful to provide more clarity on the use of a risk-based approach to ongoing CDD. HSBC would recommend that any guidance creates sufficient flexibility to support an event-based ongoing CDD model that can be supported via technological advances e.g. AI.

Introducing a timeframe or 'sinking lid' for existing (pre-Act) customers

4.71. How could we ensure that existing (pre-Act) customers are subject to the appropriate level of CDD? Are any of the options appropriate and are there any other options we have not identified? What would be the cost implications of the options?
The option of bringing pre-Act customers up to standard each time a customer change (regardless of materiality) is made or a 'sinking lid' option would be reasonable. There would need to be clarity around dormant/inactive customers and the actions a reporting entity would need to take in these circumstances. It may not always be possible to end customer relationships at this stage, particularly if the customer relationship is dormant and the funds cannot be returned.

9 Source: New Zealand Bankers Association draft submission 211118

Avoiding tipping off

4.73. Once suspicion has been formed, should reporting entities have the discretion not to conduct enhanced CDD to avoid tipping off?

Yes - it is very difficult to complete ECDD on a customer after a potentially suspicious transaction without tipping off the customer. In addition, a reporting entity may decide to terminate the business relationship on the basis that the suspicious activity reported is outside of risk appetite. It is not practical to conduct ECDD on customers in such instances.

Politically exposed persons

4.79. Do you have any challenges with complying with the obligations regarding politically exposed persons? How could we address those challenges?

Please refer to responses under question 4.1.

4.80. Do you take any additional steps to mitigate the risks of PEPs that are not required by the Act? What are those steps and why do you take them?

Ongoing screening, negative news checks to ensure that the level of risk remains within appetite

4.81. How do you currently treat customers who are domestic PEPs or PEPs from international organisations?

Similar to international PEPs, with no differentiated approach to these categories of PEPs.

4.82. Should the definition of 'politically exposed persons' be expanded to include domestic PEPs and/or PEPs from international organisations? If so, what should the definitions be?

4.83. If we included domestic PEPs, should we also include political candidates and persons who receive party donations to improve the integrity of our electoral financing regime?

4.84. What would be the cost implications of such a measure for your business or sector?

Yes, the definition should be expanded to include domestic PEPs so that the risk rationale is consistent with international PEP definitions. There are other low risk countries, similar to New Zealand, and if customers from those countries are considered higher risk merely because they are not in New Zealand, it is inconsistent from a risk standpoint. The definition should also include international organisations like UN organisations e.g. directors, deputy directors and members of the board or equivalent of an international organisation.

The level of officials in scope should be clearly defined. Domestic PEPs should include elected or appointed members of parliament and leaders/members of political parties. Domestic PEPs should not include local government officials e.g. local council staff.

HSBC internal policy does not differentiate between international and domestic PEPs so there would be no additional cost implications.

4.85. How do you currently treat customers who were once PEPs?

Declassification is permitted 12 months after the PEP has ceased being entrusted with a prominent public function, subject to the PEP meeting certain risk-based criteria e.g. no unresolved negative news, no money-laundering concerns based on the previous 6 months' activity monitoring, no longer connected to lobbying, etc.

4.86. Should we require a risk-based approach to determine whether a customer who no longer occupies a public function should still nonetheless be treated as a PEP?
4.87. Would a risk-based approach to former PEPs impact compliance costs compared to the current prescriptive approach?
A risk-based approach would be best as a reporting entity would need to determine the level of influence that the person still retains. The costs would rise as there would need to be more risk-based policies, it would require additional training for staff to understand and apply policies and then monitor them adequately.

4.88. What steps do you take, proactive or otherwise, to determine whether a customer is a foreign PEP?
Screening for all customers.

Correspondent banking

4.115. Are the requirements for managing the risks of correspondent banking relationships set out in section 29 still fit-for-purpose or do they need updating?
It would be beneficial to update some of the obligations so that it is more aligned with industry practice. Some of the obligations are difficult to meet e.g. assessing the respondent's AML/CFT controls to ascertain that they are adequate and effective and being satisfied that the respondent has verified the identity of, and conducts ongoing monitoring of, its customers. Without step-in rights, reporting entities will need to rely on data that the respondent provides e.g. its confirmation of audit results, internal monitoring, etc. There is very little scope for a bank to obtain full information on a respondent's controls and processes, especially as these may sometimes be competitors and provide limited information. If the obligations cannot be amended, it would be useful to clarify what level of assessment/verification is required. Having more clarity would make it easier to comply with the obligations.

Prescribed transaction reports

4.156. Are the prescribed transaction reporting requirements clear, fit-for-purpose, and relevant? If not, what improvements or changes do we need to make?
4.157. Have you encountered any challenges in complying with your PTR obligations? What are those challenges and how could we resolve them?
4.158. Should we issue regulations or a Code of Practice to provide more clarity about the sorts of transactions that require a PTR?
4.159. If so, what transactions have you identified where the PTR obligation is unclear? What makes the reporting obligation unclear, and how could we clarify the obligation?
The current requirements are complex, particularly given the nature of payments infrastructure. The requirements contain exclusions which are challenging to code in an automated reporting system. We would welcome a Code of Practice or more specific guidance to provide clarity on the following areas:

- Transactions facilitated via MT202s, and where funds transfers are not directly sent internationally, instead deals are made between banks and their customers in 2 separate jurisdictions in order to facilitate a trade.
- Instances where MT202s (or other similar message types) are used to facilitate funds transfers on behalf of an underlying customer. Banks have very limited ability to control messages sent to them. There are payments that might meet the SWIFT definition for use of a MT202 but not the wire transfer exclusion for a 'financial institution to financial institution' settlements where both parties are acting on their own behalf, which are complex to identify and code for. MT202s may not contain all the same information and so may not fit the PTR schema requirements.

- Credit card to credit card payments that have a cross-border element, which are not currently reported as long as the payment contains a credit card number. Credit card companies do not have the same obligations.
- Situations where financial institutions and DNFPBs are customers of other reporting entities and either initiate or receive funds on behalf of a third party. It is unclear in these instances who has the obligation to report, who the ordering institution is and who the beneficiary institution is.
- Instances where one bank considers it is acting as an intermediary institution, whereas another bank considers the receipt of funds from that bank to be a domestic wire transfer with no intermediary institution involved. Visibility of information can be an issue.
- Bulk or batched international wire transfers that are processed via SWIFT (MT103 or MT202), but underlying payment instructions are sent outside of SWIFT and payments could be considered as domestic payments.
- Payments between 2 NZ banks in a foreign currency but offshore intermediary is used to facilitate the FX requirements. It is unclear to us whether these payments are intended to be reported and whether they have any intelligence value.
- Cross-border corporate funds sweeps as part of a corporate's treasury management. It is unclear to us what the reporting expectations are here.
- ISO20022 implications for PTR. Regulation and guidance need to align to new industry payment structures.
- It is unclear to us what the reporting expectations are for Nostro account settlements.[10]

HSBC is supportive of adopting a 'First In, Last Out' methodology to determine who is responsible for prescribed transaction reporting as we believe this provides more clarity to the reporting entities on some of the above issues.

Reliance on third parties

4.171. Do you use any of the reliance provisions in the AML/CFT Act? If so, which provisions do you use?

Yes, section 34.

4.173. Are there any changes that could be made to the reliance provisions that would mean you used them more? If so, what?

If section 34 could be clarified further in terms of the minimum standards that agents must meet for record-keeping requirements and transfer of information, it would be helpful. E.g. all records must be transferred to the reporting entity within 5 business days of establishing a business relationship, etc.

4.174. Given the "approved entities" approach is inconsistent with FATF standards and no entities have been approved, should we continue to have an "approved entities" approach?

No, there is no merit to having approved entities in the legislation if there is no list of entities for New Zealand.

4.175. If so, how should the government approve an entity for third party reliance? What standards should an entity be required to meet to become approved?

Potentially, entities who sign up and have satisfactory independent audit results or onsite inspections (for reporting entities). However, this would raise questions around what happens if an entity has material observations at an audit/inspection or if it chooses to de-register itself. Would the prior CDD conducted by the entity need to be reviewed/re-done by the reporting entities relying on it or would

10 Source: New Zealand Bankers Association draft submission 211118

there be 'good-faith' protections for the reporting entities? The level of liability shared between the reporting entity and the approved entity would be another factor for consideration. There may be additional concerns around privacy/data-sharing, needing to obtain explicit customer consent, keeping customers updated, etc. which might be onerous for entities.

4.176. If your business is a reporting entity, would you want to be an approved entity? Why or why not?
No, please refer to the response under question 4.175.

4.177. Are there any alternative approaches we should consider to enable liability to be shared during reliance?
Sharing liability would not always work for reporting entities who rely on agents in other countries. For domestic reliance, obligations for agents/third parties to provide CDD requirements according to the Act would help.

4.182. Should we issue regulations to explicitly require business to do the following before relying on a third party for CDD:
• consider the level of country risk when determining whether a third party in another country can be relied upon;
take steps to satisfy themselves that copies of identification data and other relevant documentation will be made available upon request without delay; and
• be satisfied that the third party has record keeping arrangements in place.
Yes, this would be beneficial. It is expected that most reporting entities would include this in their contract with third parties anyway; however, would be useful to include in regulations.

Compliance officers

4.188. Should the Act mandate that compliance officers need to be at the senior management level of the business, in line with the FATF standards?
No, this may cause difficulties for reporting entities that are part of larger group companies. The group company may consider certain staff to be senior management based on the job grade they hold rather than the role they play in the country. This would make it difficult to comply with the legislation or may require ministerial exemption applications for the compliance officer (due to their job grade) to be based offshore. Retaining the requirement at the current level where the compliance officer has to report to a senior manager provides more flexibility while allowing for adequate levels of seniority.

Review and audit requirements

4.192. Do we need to clarify expectations regarding reviewing and keeping AML/CFT programmes up to date? If so, how should we clarify what is required?
It may be useful to specify the minimum frequency of updates to the programme. While most reporting entities will review this annually, some may review it less frequently. This does not mean that the programme is not effective; it may mean that reporting entities update the underlying policies and procedures and the trigger to update the overall programme is less frequent.

4.193. Should legislation state that the purpose of independent audits is to test the effectiveness of a business's AML/CFT system?
Yes, it would be very beneficial for the Act or regulations to state the intent of independent audits. If it could cover the key points that must be tested, it would also be useful e.g. effectiveness of transaction monitoring. At present, each auditor interprets it differently and results are varied. There is inconsistency both in the scope and depth of audits and some areas that do not require detailed focus are covered (e.g. observations about whether the programme contains references to all sections of the Act) while others (e.g. transaction monitoring) which are more critical are not covered in sufficient detail. It should be noted that any change in the requirements may cause auditors to

increase their fees and may result in a corresponding increase in compliance costs for reporting entities who cannot rely on their internal audit function.

4.194. What other improvements or changes could we make to the independent audit or review requirements to ensure the obligation is useful for businesses without imposing unnecessary compliance costs?
Defining minimum standards for auditor competence would help. If auditors were supervised/governed in some manner, it would also help.

Auditors are sometimes unaware of guidance provided by supervisors to reporting entities. Supervisors may have different interpretations of regulations/guidance and the same auditor might not be able to audit two reporting entities in a similar manner. Additionally, each auditor's interpretation of legislation/regulations is different and this often results in different interpretations of meeting obligations.

Suspicious Activity Reporting

4.203. How can we improve the quality of reports received by the FIU and avoid low-quality, defensive reporting?
HSBC would welcome more direct and regular feedback from the FIU on intelligence provided to them e.g. what reports are useful or not. This would help banks to further enhance their internal monitoring capabilities to detect illicit activity.

Sharing SARs or SAR information

4.206. Should we expand the circumstances in which SARs or SAR information can be shared? If so, in what circumstances should this information be able to be shared?
Yes - for multi-jurisdictional entities, SAR information (not SARs) should be able to be shared with intra-group entities for risk management purposes and reviewing the customer relationship across geographies.

4.207. Should there be specific conditions that need to be fulfilled before this information can be shared? If so, what conditions should be imposed (e.g. application to the FIU)?
HSBC would recommend that the details of why information needs to be shared, in what circumstances it will be shared, how and where the data will be held, the class of persons who will have access to the data, how unauthorised access/disclosure will be maintained, etc. be documented as part of the AML/CFT programme.

Use of technology to improve regulatory effectiveness

5.13. What challenges or barriers have you identified that prevent you from harnessing technology to improve efficiencies and effectiveness? How can we overcome those challenges?
Please refer to responses under question 4.1 relating to Digital ID & Ultimate Beneficial Ownership.

As a general comment, the existing rules to manage financial crime risk were not prepared with current and future technology in mind. HSBC believes that a more risk-based approach (vs. rules-based approach) facilitates the greater use of technology to enhance financial crime risk management.

Changes to the Act/regulations or new regulations to be released

6.1. What are your views regarding the minor changes we have identified? Are there any that you do not support? Why?

1. Failing to submit an annual report to an AML/CFT supervisor is a civil liability act
   It would be useful to clarify whether the civil liability extends to late submissions or inaccurate submissions as well.
2. Amend section 58(2) to ensure that a business' risk assessment reflect government advice about national and sectoral risks. Further clarity on this change would be beneficial. Reporting entities refer to the national and sectoral risks when preparing their AML/CFT risk assessments; however, their assessment of the risks may differ based on the products/services they offer. It is unclear whether this change would result in a less risk-based approach where reporting entities would be required to reflect the NRA/SRA risk ratings/rationale in their AML/CFT risk assessments without considering individual business offerings.
3. Issue a regulation which states that simplified CDD is not appropriate where money laundering or terrorism financing risks are high or if there is suspicion of ML/TF. It would be useful if further clarity could be provided in terms of the instances where this could apply. If a customer qualifies for simplified CDD, the inherent risk of ML/TF is presumed to be low and minimal CDD is completed to identify any further risks. If any risks are identified through account monitoring or SARs, the risks are addressed at that stage of the process which is covered by the Act.
4. Amend section 52 to clarify that records must be made available immediately (e.g. upon request from a supervisor). It would be useful to specify the time period within which records must be made available e.g. 5 working days from request being received. This is to allow reporting entities to update their agreements with agents/third parties who may complete CDD on their behalf.
5. Require ordering institutions to keep records on beneficiary account number or unique transaction numbers. It would be useful to specify the timeframe for retention of this information e.g. if the standard 5-year period applies or whether a shorter timeframe is applicable.

6.2. Are there any other minor changes that we should make to the Act or regulations?

It is unclear how the data in the AML/CFT annual report is used by supervisors to monitor reporting entities. Reporting entities provide a large amount of data, often requiring substantial systems investments and manual reporting to be able to provide the information requested. It would be beneficial to review the content of the report to understand if the information is useful to the supervisors and how it aids in either managing financial crime or supervising reporting entities. If the information is not materially significant to either purpose, it could potentially be reduced to fewer, more critical data elements. Data for a representative period could also be used e.g. data for one quarter of the year rather than a full one-year period. These changes may be more cost and resource efficient for both reporting entities and supervisors.