

BnEI 2.0

Audit Guidance Manual

CONTENTS

1	Governance	4
1.1	Scope	4
1.2	Roles	5
1.3	Audit Principles.....	6
1.4	Audit process guidance	10
1.4.1	Audit Scope Form	10
1.4.2	Pre-audit diagnostic and scoping agreement.....	10
1.4.3	Conducting the audit and audit outcome	10
1.4.4	Letter of Confirmation and re-audits	11
1.4.5	Revision of the BnEI Framework and Manual	11
2	Baseline CMS Principles.....	12
2.1	Governance, Oversight & Autonomy	12
2.2	Risk Assessment	14
2.3	Policies and Procedures	15
2.4	Policy Implementation & Incentivization	16
2.5	Issue Management & Investigation.....	17
2.6	Monitoring & Testing	18
3	Risk Assessment	20
3.1	Risk assessment on sales and commercial intermediaries	20
3.1.1	Criteria	20
3.1.2	Intermediary Risk Assessment Models	20
3.1.3	Mitigation measures.....	21
3.2	Check list – hiring former government official or PEP	26
3.2.1	Risk criteria	26
3.2.2	Mitigating measures.....	26
4	Minimum standards	28
4.1	Commitment from Senior Management (#4)	28
4.2	Compliance Policies and Procedures (#8)	29
4.3	Risk Assessment (#4)	31
4.4	Training and Continuing Advice (#6)	33
4.5	Third Party Management (#6)	34
4.6	Confidential Reporting, Internal Investigation and Disciplinary Measures (#4)	35
4.7	Continuous Improvement and Review (#2)	36
5	Annexes	39

5.1 Definitions	39
5.2 Audit Scope Form	41
5.3 Document Request List	43
5.4 Interview List	49
5.5 Sampling Guide.....	50
5.6 Annual Letter of Confirmation	51

1 GOVERNANCE

1.1 SCOPE

Supplementary to the BnEI Code of Ethical Business practice¹, this guideline describes risks in the context of anti-bribery and anti-trust alongside more specific risks for the banknote sector and mitigation measures to be implemented by applicants/members of the BnEI.

This document outlines the framework and shall be used as an audit guidance manual (the “Manual”) by the assessors and each applicant/member. The scope of the audit includes the organisation’s business units carrying out banknote activities, at minimum the head office. At the request of the applicant/member, it can also encompass additional business units. All higher risk subsidiaries that hold their own direct contracts with customers, service providers, or intermediaries are fully included in the scope of the audit².

Banknote activities include, but are not limited to:

- Sale of banknotes or related products and services such as paper, ink, machinery, and security features;
- Service provisions related to banknote design, production or handling;
- Contracting for banknote-related projects or operations;
- Lobbying within the banknote industry;
- Engineering of banknote production, security features, or related technology;
- Logistics involved in the transportation and secure handling of banknotes or related products.

The BnEI audits should be conducted remotely for interviews and document review, absent special circumstances.³ New applicants must have their first audit completed in person at the office of the applicant’s choosing. Where the member disagrees with the decision of the assessor for an in-person audit or the assessor disagrees with the selected office, then the member can appeal to the Accreditation Council for a final decision to be made. Any additional sites to be included in the audit will be audited remotely.

An audit cycle typically consists of 3 years (see section 1.3 Audit Principles). Taking a risk-based approach, the assessors will also include (onsite or not) 50% of key sites in scope of the audit in a period of 2 audit cycles and in addition to the head office based on the risk profile. In order to determine the scope of the audit, consideration will be given to, for example:

- The size and complexity of the organisation;
- Where employees in key business functions are based;

¹ https://www.bnei.com/wp-content/themes/bneidesign/downloads/BnEI_Code_of_EthicalBusinessPractice.pdf

² Subsidiaries that represent a higher risk (e.g. because of direct contact with customers, service providers or intermediaries) should be identified by each applicant/member and included in the scope. The other subsidiaries can be included in the audit voluntarily (applicant/member’s decision).

³ Special circumstances may include situations where the assessor has justified concerns about the applicant’s/member’s compliance with the BnEI standards, when the assessor reasonably determines that a remote audit will constitute a risk to the quality or effectiveness of the audit based on failure of preparation of the member (e.g. insufficient digitized documents, inability to access interviewees), or where the member considers that an in-person audit will afford a better opportunity to leverage the experience of the assessor. If an in-person audit is desired or required, the BnEI audit will be conducted in person at the office selected by the member.

-
- Where key banknote activities take place;
 - The size of each site; and
 - Whether there are high risk sales and commercial intermediaries or other relevant external stakeholders managed from those sites.

In cases where anti-bribery and anti-trust management systems are designed and implemented centrally, assessors will focus primarily on the head office and conduct sampling into the different sites on a risk basis. Similarly, if policies and records reviewed are typically applicable to the company as a whole, site-specific variations will be reviewed on a risk basis. In conducting the audit procedures, the assessors look into several relevant functional areas of the business – including but not limited to compliance, finance, sales, procurement and human resources. As a result, the assessors might need to look into operations distributed across the territories where the company has relevant organisational functions⁴, to get a view on the control measures the organisation has in place to reduce the risk of bribery, corruption and non-compliance with anti-trust regulations.

If assessors do not physically visit a particular site, they may nevertheless conduct remote interviews or document reviews, for example related to decentralized sales hubs where commercial activities are managed independently from the head office. Additionally, if parts of the anti-bribery or anti-trust system are managed from regional sites, for example with local compliance officers or key management functions, assessors would interview relevant employees at those regional sites.

The accreditation is awarded to the company as a whole and not to individual sites or subsidiaries or locations. The subsidiaries or locations covered by the review are listed in the audit report and will be transparent for the Accreditation Council.

In accordance with the process in Section 9.1.3 of the BnEI Constitution, where a member or an intermediary of the member has been found to have committed an AB & AT offence for the benefit of the member by a competent authority who adheres to principles of natural justice, the member will be disqualified from BnEI membership in accordance with the BnEI constitution for a period of three (3) years and may reapply for membership after this period. The final decision of the General Assembly will be publicly published.

1.2 ROLES

The applicant/member facilitates the renewal of its accreditation and provides support to the assessor promptly and effectively throughout the audit process. Activities to be performed in this context can entail (not exhaustive):

- Completing the Audit Scope Form⁵ providing accurate organisational information;
- Providing relevant documents as requested by the assessor via the Document Request List⁶, sample selections and further clarifications;
- Facilitating the scheduling of the interviews with internal and external stakeholders⁷;
- Reviewing the draft audit report and providing management response and actions; and
- Completing Annual Letter of Confirmation⁸.

⁴ Relevant organizational functions consisting of operations, finance and accounting, sales, legal & compliance and procurement.

⁵ Included in Annex 5.2 Audit Scope Form.

⁶ Included in Annex 5.3 Document Request List.

⁷ Included in Annex 5.4 Interview List.

⁸ Included in Annex 5.6 Annual Letter of Confirmation.

An external audit is conducted by the appointed assessors (one of the selected firms) and will be performed on all sections of this Manual at least every three years (the 'audit cycle'). The assessor is responsible for executing audits and plays a critical role in assessing the adequacy and effectiveness of the compliance management system, and anti-bribery and anti-trust measures. The assessor's role also includes ensuring that the audit process is conducted objectively, independently, and impartially. A report will be delivered as a result of the audit and will be presented to the Accreditation Council.

The Accreditation Council will ultimately decide whether to award the BnEI accreditation to the company, or not, supported by the results of the audit. The consequences of this decision, whether positive or negative, will take effect 7 days after the Accreditation Council issues it. The member maintains its previous accreditation status until a new decision is issued by the Accreditation Council.

In case of dispute between the assessors and the applicant/member, the Accreditation Council can be involved in the dispute resolution process at the request of the applicant/member (referring to the Terms of Reference of the Accreditation Council). The Accreditation Council will have no liability to either party for any decision made by the Accreditation Council in such dispute resolution process.

1.3 AUDIT PRINCIPLES

The assessors will evaluate the AB & AT framework as detailed in the BnEI 2.0 Manual, leading to a total of respectively **46 points** and **38 points** to be awarded for **non-ISO37001** and **ISO37001 accredited members**. The BnEI audit will be executed combining three audit techniques:

- Interviews with managers, employees or other relevant internal and external stakeholders;
- Review of requested policies, procedures and other key documents; and
- Effectiveness testing based on samples selected from the total population.

The assessors will evaluate the following three aspects of the BnEI Framework implemented by the applicant/member in a sequential order:

- a. Baseline compliance management system ('CMS') principles (see section 2):

The assessors will evaluate the CMS implemented by the applicant/member following six audit topics:

1. Governance, Oversight & Autonomy
2. Risk Assessment
3. Policies & Procedures
4. Policy Implementation & Incentivization
5. Issue Management & Investigation
6. Monitoring & Testing

If the applicant/member is not ISO37001 certified: The 12 baseline CMS principles (elaborated in Section 2 of this Manual) will be evaluated to ensure the minimum requirements of an anti-bribery and anti-trust compliance management system are designed and implemented. Sample-based tests will be conducted by the assessors where relevant to verify the effectiveness of the implementation. Please note that in the few cases where duplications in the what to test and/or how to test sections occur the applicant/member will, if necessary, only be marked down on one of these points.

Each of the CMS principles in scope of the audit will be awarded an individual Pass or Fail score. This will result in a “Pass” (12 out of 12 Pass grades), “Improvement Needed” (10 or 11 out of 12 Pass grades), or “Fail” grading (9 out of 12 Pass grades or less). Only in case of a “Pass” or “Improvement Needed” grading, the applicant/member will have the opportunity to become accredited. In case of a “Fail” grading, the applicant/member can reapply for accreditation within six months after the results from the Accreditation Council were received. However, at the applicant/member’s request, the assessors can continue with the audit to gain insight into the areas for improvement.

If the applicant/member has obtained an ISO37001 certification by an accredited auditor⁹: A first-time applicant to the BnEI organization will be fully assessed on all 12 principles as above. After this, a risk-based selection of 4 out of 12 baseline CMS principles will be reviewed based on the ISO37001 Auditing Standard to verify that the certification has been obtained in a qualitative manner, by an accredited auditor. A selection will be made by the assessors which 4 elements will be part of the review. This might vary between organisations and audit cycles. Also, in order to ensure that the system has been implemented on all relevant local levels, assessors might select subsidiaries or business units as well. Sample-based tests will be conducted by the assessors where relevant to verify the effectiveness of the implementation.

Each of the CMS principles in scope of the audit will be awarded an individual “Pass” or “Fail” score. This will result in a “Pass” (4 out of 4 Pass grades), or “Fail” grading (3 out of 4 Pass grades or less). Only in case of a “Pass”, the applicant/member will have the opportunity to become accredited. In case of a “Fail” grading, the applicant/member can reapply for accreditation within six months after the results from the Accreditation Council were received. In that case, the audit will follow the methodology applied for not ISO37001 certified members meaning that all 12 baseline CMS principles will be evaluated. At the member’s request, the assessors can continue with the audit to gain insight into the areas for improvement.

b. Risk Assessment for banknote specific risks (see section 3):

Complementary to the generic success factors of a compliance management system, banknote specific risks have been identified. The BnEI Annual Meeting will review the list and update it as required. As of January 2026, those areas are:

- working with sales and commercial intermediaries; and
- hiring former government officials or PEPs.

For these risk domains, the assessors will assess the risk assessment completed by the applicant/member to ensure that risk gradings have been applied in an appropriate way regarding design and effectiveness and that the relevant mitigating measures are implemented in a way to combat the risks. The applicant/member will provide evidence on how the risks are assessed and mitigated. The grading will be based on the assessor’s evaluation, providing a contextual analysis of the measures implemented and based on the member/applicant’s documentation per risk assessment. The following elements will be considered per risk domain and awarded a “Pass” or “Fail” grading:

- Relevance of the criteria of the applied risk assessment methodology

⁹ This is also applicable for matrix certifications (on Group level).

- Completeness and correctness of applied methodology across the population (sample-based test)
- Completeness and correctness of applied mitigation measures across the population (sample-based test)

Consequently, each applicable risk assessment will be graded with a “Pass”, “Improvement Needed” or “Fail” score. Only in case of a “Pass” or “Improvement Needed” grading, the applicant/member will have the opportunity to become accredited. At the applicant/member’s request, the assessors can continue with the audit to gain insight into the areas for improvement.

The “3.1.2. Intermediary Risk Assessment Model” provides a minimum standard for compliance. Members/applicants must at least meet these criteria to demonstrate BnEI compliance. Members/applicants are at liberty to apply a more stringent methodology.

The applicant/member must provide evidence to the assessor that at least full mitigation measures as required by the standard and based on the risk assessment have been implemented across the full population. The assessors will then evaluate whether the mitigating measures have been effectively implemented.

A “Fail” grade will be issued if the mitigation measures are found to be insufficient and/or incorrectly applied.

The assessor may recommend additional mitigation measures as best practice enhancements. These recommendations are advisory and do not impact the final “Pass” or “Fail” determination.

In case of a “Fail” grading, the applicant/member can reapply for accreditation six months after the results from the Accreditation Council were received.

The risk assessment framework is expected to be in place by the time of the first audit. Regarding mitigation measures, a transition period of three years from the adoption of the Manual by the membership will be permitted for implementation. During this period, the assessor will evaluate during the applicant/member’s audit whether a credible plan to achieve full compliance has been developed for full implementation from year three of the Manual. Full implementation of the mitigation measures will be required starting in year three from publication of this Manual.

As for the full audit report, the Accreditation Council can be involved in case of disagreement between the assessors and the applicant/member at the request of the applicant/member (referring to the Terms of Reference of the Accreditation Council).

- c. Minimum Standards (see section 4):
- All 34 minimum standards will be assessed and awarded 1 point if implemented where a minimum of 80%¹⁰ needs to be achieved in the first year after approval of the Manual.
 - This will increase with 5% per year until a 90% implementation rate is set as requirement.
 - This means that out of 34 minimum standards, 27 standards must be implemented to obtain a “Pass” grading in the first year after approval of the BnEI 2.0 standard. Afterwards, this will increase to 31.

¹⁰ In this case, the Annual Letter of Confirmation will be leveraged to ensure that the necessary steps are taken to move to a 90% pass rate.

- An applicant/member cannot pass where there is more than 1 missing standard in each of the categories of section 4 (ie. 4.1, 4.2, 4.3, etc).

Until the applicant/member has reached the target of 90%, a partial re-audit will be performed on a yearly basis.

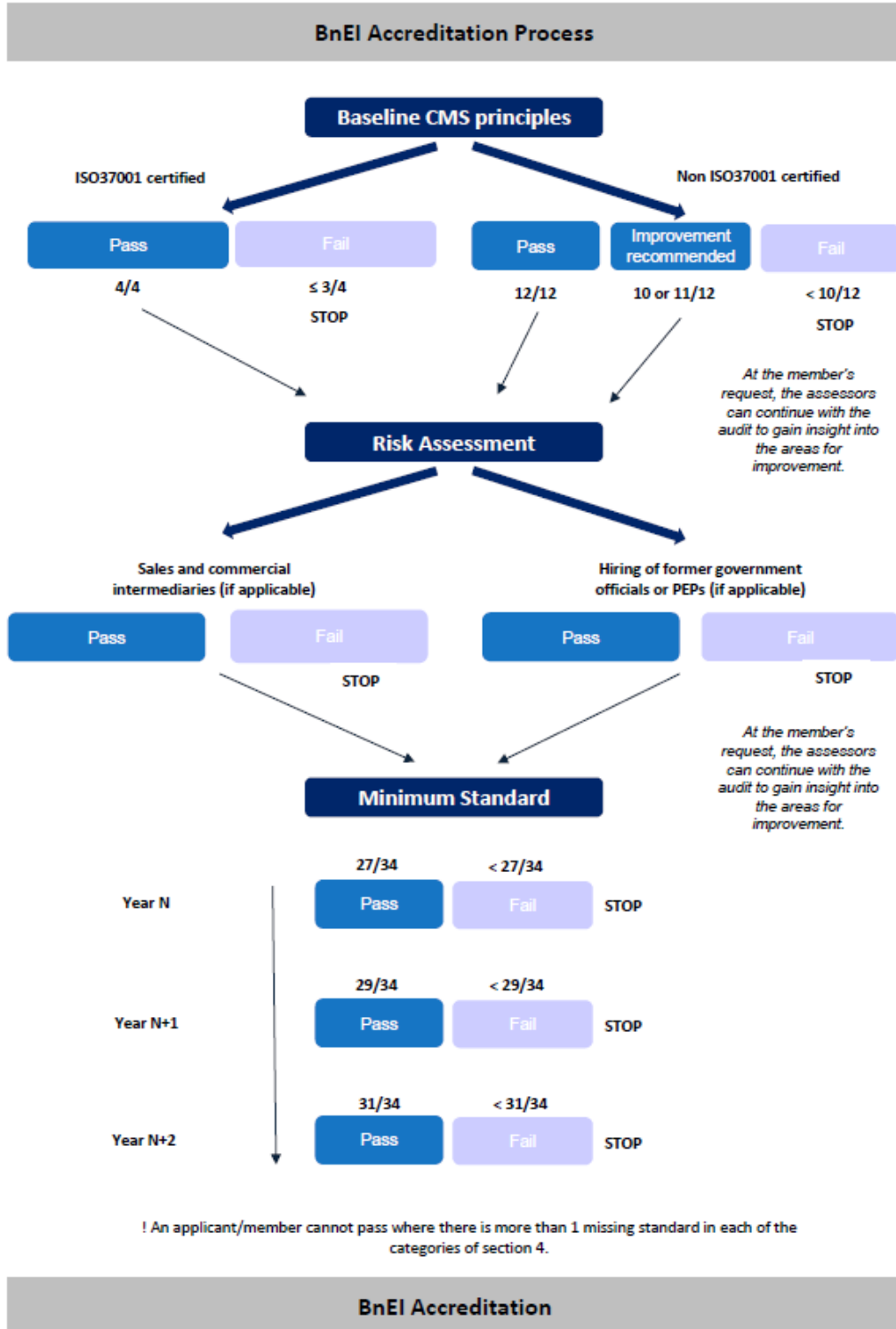


Figure 1: new accreditation process

1.4 AUDIT PROCESS GUIDANCE

1.4.1 Audit Scope Form

In case of a new applicant to BnEI, BnEI will send the audit scope form (Annex 5.2) that needs to be completed by the applicant to provide a preliminary view to the assessors concerning the number of entities, sales and commercial intermediaries, an ISO37001 certification, etc.

In case of existing BnEI members, the member shall proactively communicate any changes to the member's most recent scoping form before the start of the audit to renew the accreditation.

1.4.2 Pre-audit diagnostic and scoping agreement

If requested by the applicant, a pre-audit diagnostic can be conducted by the selected assessor to give a first view on the readiness of the applicant to apply for the BnEI accreditation in the short term. This is a high-level assessment consisting of meetings and document reviews and results in a short form report.

In any case, an engagement letter between the assessor and the applicant will be drafted based on the information in the audit scope form before starting the audit procedures.

1.4.3 Conducting the audit and audit outcome

Once the engagement letter is signed between the assessor and applicant/member, the audit process will be kicked-off, including the following actions:

- Schedule pre-audit preparation meeting;
- Agreement on timing of the audit activity:
 - For existing BnEI members, this shall be considering the due date of the Accreditation Council and expiry date of the previous accreditation (final report dates should be used to define timeline);
- Agreement on onsite/remote work;
- Assessors provide document request list, to be compiled and delivered by the applicant/member in a timely manner.
- Assessors to provide list of interviewees, including possible substitutes agreed to by the applicant/member should interviewees be unavailable at the specified times, and interview times will be set by the applicant/member during the audit process.

The assessors will undertake the audit during the agreed upon dates and based on the documentation and information provided. All conclusions will be formulated in a full report for review by the applicant/member, and management responses and action plans will be formulated by the applicant/member in case of any "Fail" gradings. In the case of any "Fail" grade, the report by the assessor will specify the deficiencies that warrant a "Fail" grade. The applicant/member will have a maximum of 10 weeks from receipt of the draft report from the assessor to remediate any potential "Improvement Needed" or "Fail" gradings and satisfy the assessor the remediation is complete.

Following the conclusion of the remediation period stated in the previous paragraph, the full report, adjusted to reflect any completed remediation, will be confidentially shared with the Accreditation Council at least one week before the meeting with the Accreditation Council. The assessors will present their conclusions and answer any remaining questions of the Accreditation Council, and the Accreditation Council will consider all information to make their final decision whether to award

accreditation or not. Afterwards, the Chairperson of the Accreditation Council will inform the BnEI Chairperson of the outcome, who will notify the applicant/member of the decision.

1.4.4 Letter of Confirmation and re-audits

In case of a denial of accreditation, the applicant/member can reapply for accreditation no earlier than six months after the results from the Accreditation Council were received to provide sufficient time for adjustments to be made by the member.

In case of a consistent “Pass” grading across all audit aspects, the audit will be performed every three years. This will be combined with an Annual Letter of Confirmation to ensure no major changes impacted design and effectiveness of the compliance management system.

In case of “Improvement Needed” grading throughout the audit (in one or multiple aspects), a partial re-audit will be performed in the year N+1 to ensure the required mitigation measures were taken.

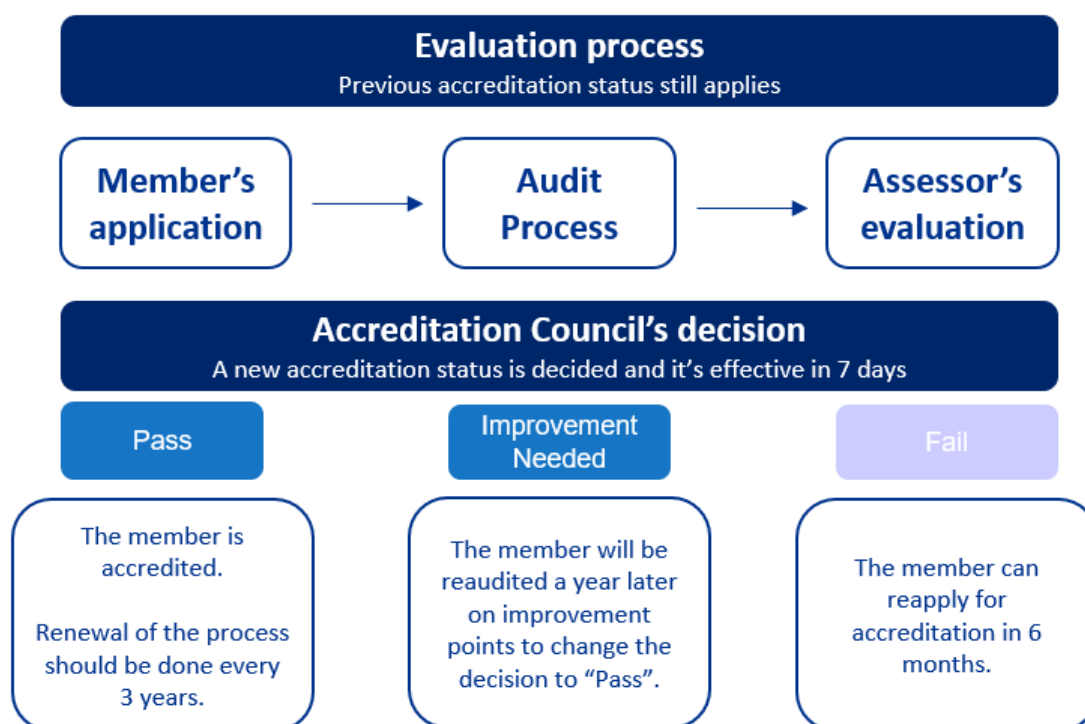


Figure 2: accreditation process timeline

1.4.5 Revision of the BnEI Framework and Manual

During the yearly members meeting, a review of the Manual must be conducted to incorporate any necessary changes or additions, and to ensure that the two remain consistent and up to date. Changes in relation to ISO may also lead to modifications in the CMS Baseline Principles.

2 BASELINE CMS PRINCIPLES

In this second section of the Manual, the minimum baseline principles of an effective anti-bribery and anti-trust compliance management system ('CMS') are outlined. These will be evaluated by the assessors on design and implementation:

2.1 GOVERNANCE, OVERSIGHT & AUTONOMY

1. The CMS shall be in line with legal requirements, organisational context (including business model, size, structure, locations) and expectations of its stakeholders and shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the objectives.

What To Test

- That a CMS is established, documented and proportionate to the organizational context and in line with stakeholder expectations.
- That the CMS includes mechanisms to identify, document, and update legal requirements relevant to the organization.
- That the purpose and objectives of the CMS are clear and internal and external issues are identified to update the CMS.

How To Test

- Interview the *compliance officer (or equivalent)* to understand the purpose and scope of the CMS, and the process of scoping, identifying legal obligations and stakeholder expectations, and defining and updating the CMS and underlying policies.
 - The CMS is presented to the assessors and considers the appropriate purpose, objectives, scope, legal requirements, and stakeholder expectations and no key compliance issues have been overlooked.
 - Review past compliance issues, if any, to confirm that all key risks have been identified and that any have been resolved.
2. Senior Management shall demonstrate commitment by establishing and reviewing the CMS and its underlying elements (policies, procedures, resources) and ensuring proper integration on different levels in the organisation by promoting the right (speak-up) culture and undertaking regular communication initiatives (to Governing Committees in the organisation). Senior management shall ensure the organisation promotes this to its customers.

What To Test

- That senior management makes a commitment regarding compliance, which is supported by a documented review of the CMS and underlying policies.
- That senior management promotes a speak-up culture within the organization.
- That proper integration of the CMS can be demonstrated by communication initiatives to governing committees and customers.

How to test

- Interview *members of senior management* on their understanding and commitment concerning the CMS, and how a speak-up culture is promoted.
 - Verify that a review of the CMS and its underlying policies by senior management is performed and documented (e.g. through meeting minutes or policy sign-off or statements).
 - Verify that the CMS is regularly updated based on stakeholder analysis, risk assessment, and periodic updates to ensure alignment with compliance objectives.
 - Verify that evidence exists that a speak-up culture is actively promoted (e.g. via the intranet, policies, training).
 - Review documented communications (e.g., presentations) regarding the CMS that have been shared with governing committees and, where applicable, customers.
3. A compliance function shall be established with adequate resources to oversee the design and implementation of the CMS, provide guidance, and conduct monitoring and oversight on conformity with AB & AT requirements, based on company policy and legal standards. Appropriate reporting lines shall be established, and a clear delegation of authorities shall be put in place. While large companies may find it convenient and cost effective to have a dedicated compliance function, smaller companies may have compliance functions embedded within other departments, such as legal, finance or security, provided they are independent from commercial functions,¹¹ are free from any conflicts of interest, and have direct access to senior management.

What to test

- That the compliance function (or equivalent) has enough resources to oversee the CMS and ensure conformity with AB & AT requirements.
- That the compliance function (or equivalent) has a dotted line/access to the top management and is independent from commercial functions and free from conflict of interest.

How to test

- Interview the *compliance officer (or equivalent)* to discuss their remit, workload, reporting lines and any areas of concern they may have regarding resourcing, particularly regarding regional support in high-risk areas.
- Interview the *compliance officer (or equivalent)* to assess whether any conflict of interests occurred and how this is being dealt with.
- Review the compliance officer (or equivalent)'s job description, organization chart and the function's budget to confirm that the compliance officer (or equivalent) is operating independently.

¹¹ Commercial functions include roles which may experience a conflict of interest between AB/AT risk prevention and obtaining a business opportunity for the applicant/member. This includes, but is not limited to, individuals involved in business development, sales, and customer relations. Innovation, and research and development roles will fall into this category where they are in a role that includes negotiation and decision making on pricing and contract terms.

- Review relevant policies and procedures to verify the compliance function's responsibility to oversee the design and implementation of the CMS, provide guidance, and conduct monitoring and oversight on conformity with AB & AT requirements.
- Review that there is a clear process for reporting and escalating AB & AT compliance issues.

2.2 RISK ASSESSMENT

4. The organization needs to regularly identify, assess, and evaluate the bribery and anti-trust risks including the existing mitigating measures.

What to test

- That the risk management processes are carried out fully and take proper account of bribery and anti-trust risks, covering all activities and markets, and the existing mitigation measures.
- That the organization monitors and reviews the effectiveness of its risk mitigation measures for bribery and anti-trust risks.

How to test

- Interview the *risk manager (or equivalent)* or *compliance officer (or equivalent)* to assess the processes for identifying and monitoring bribery and anti-trust risks and mitigation measures.
- Review that the risk assessment is documented and includes relevant bribery and anti-trust risks and controls.
- Check for evidence of periodic risk assessment (report, meeting minutes, etc.).
- Review monitoring and evaluation reports to confirm that risk mitigation measures are regularly assessed.

5. Regarding gifts, hospitality and travel transactions, the organization shall assess the bribery risk and take relevant mitigating measures.

What to test

- That there is a process established to assess the bribery risk regarding gifts, hospitality and travel transactions.
- That relevant mitigation measures are established and implemented.

How to test

- Interview the *compliance officer (or equivalent)* to understand relevant processes to assess risks regarding gifts, hospitality and travel transactions and how proper mitigation measures are designed and implemented.
- Review that the process to assess bribery risks related to gifts, hospitality and travel is documented and includes an approach to install relevant mitigation measures depending on the risk assessment outcome.

-
6. Procedures shall be implemented to ensure sales and commercial intermediaries commit to prevent any AB & AT risks. Appropriate steps should be taken to ensure that AB & AT risks are identified and mitigated, if needed, and that if risks cannot be mitigated to an acceptable level, relationships with intermediaries shall be terminated.

What to test

- That procedures are established to ensure that bribery risks in relation to sales and commercial intermediaries are identified, and that intermediaries explicitly commit to prevent bribery risks.
- That, if not possible to mitigate the risk, the relationship is terminated.

How to test

- Interview the *sales director (or equivalent)* to assess the awareness of bribery and anti-trust risks in relation to sales and commercial intermediaries and verify whether any relationships have been terminated considering the lack of mitigation measures.
- For a sample of active sales and commercial intermediaries, verify that there is a formal commitment (e.g. contract, compliance declaration) that they prevent any AB & AT risks.
- Review monitoring and evaluation reports to confirm that risk mitigation measures are regularly assessed.

2.3 POLICIES AND PROCEDURES

7. Policies regarding anti-bribery, anti-trust, gifts, hospitality & travel, sponsorships, donations, whistleblowing, forced labor, facilitation payments, political contributions, conflict of interest and dealing with competitors, government officials or sales and commercial intermediaries.

What to test

- That relevant compliance policies exist detailing the relevant scope and field of application.
- That the organization has implemented the established policies across all its banknote business units worldwide.
- That documented information is controlled to ensure it is secure, accessible and up to date.

How to test

- Interview the *compliance officer (or equivalent)* to understand how policies are established in relation to the CMS.
- Verify that policies exist for the following themes: anti-bribery, anti-trust, gifts, hospitality & travel, sponsorships, donations, whistleblowing, forced labor, facilitation payments, political contributions, conflict of interest and dealing with competitors, government officials or sales and commercial intermediaries.
- Review supporting documentation to confirm that relevant legal requirements and industry best practices are considered by the organization in establishing and updating their policies.

- Review implementation plans or records to confirm that the policies have been communicated to all business units.
- Review the organization's document management system to confirm that the policies are stored and accessible.
- Review the CMS policies and procedures to confirm they are applicable for the entire organization.

2.4 POLICY IMPLEMENTATION & INCENTIVIZATION

8. The organisation shall implement a process to ensure compliance with policies for all employees and, in case of high risk functions, shall conduct due diligence before employment and when the employee moves into higher risk functions. High risks functions might include people operating in the activities detailed in the "Scope" chapter of this framework and involved in decision-making process or sales and customer facing activities.¹² Performance incentives shall be considered to reduce the AB & AT risks. Those incentives can for example include completion of AB & AT trainings, compliance declarations and other initiatives as a requirement for the annual performance evaluation or (monetary) recognition awards for teams or individuals who constantly demonstrate compliance and a proactive AB & AT stance. Employee remuneration, especially for sales employees, shall be appropriate and justified.

What to test

- That the organization has implemented a process to ensure compliance with policies for all employees.
- That the requirements for deciding when to carry out due diligence on (potential) employees (or equivalent¹³) are robust and are applied.
- That the annual performance evaluation includes completion of AB & AT trainings, compliance declarations, or other compliant behavior.
- That for sales employees, remuneration is balanced and justified (e.g. fixed versus variable remuneration).

How to test

- Interview the *compliance officer (or equivalent)* to assess:
 - the implementation of the process to ensure compliance for all employees,
 - verify due diligence practices for high-risk functions, and
 - evaluate the integration of performance incentives to mitigate AB & AT risks.
- Interview the *human resource manager (or responsible department manager)* to understand the selection process, annual performance evaluation process and incentive considerations for employees working in sales to ensure employee remuneration is appropriate and justified.
- Review the CMS policies and procedures to confirm they include compliance requirements for all employees.

¹² This definition is context-dependent and should be tailored to the member/applicant's specificities.

¹³ Also including interim staff, full time consultants, freelancers and other types of staffing.

- Review the due diligence procedure for (potential) employees and verify that relevant checks and balances are being done to assess the AB & AT risks, and that appropriate measures are taken.
- For a sample of high-risk function employees, verify that due diligence was conducted prior to onboarding and no red flags were identified. If there were red flags, check that these were properly mitigated before hiring.
- For a sample of sales employees, verify that their annual performance evaluation considers AB & AT risks, and that their remuneration is balanced and justified in accordance with the company policy.

9. AB & AT policies shall be communicated to employees and sales and commercial intermediaries. Training shall be provided to employees on a regular basis, and according to the risk assessment detailed in section 3.1, to sales and commercial intermediaries.

What to test

- That all employees and sales and commercial intermediaries have access to AB & AT policies.
- That training is provided regarding AB & AT to employees on a regular basis.
- That sales and commercial intermediaries receive training which is appropriate to the risks associated with their services. (cf. Banknote specific risk assessment – Sales & Commercial intermediaries)

How to test

- Review that all internal employees can access all relevant AB & AT policies.
- Review that sales and commercial intermediaries have been provided with all AB & AT policies. (cf. Banknote specific risk assessment – Sales & Commercial intermediaries).
- Review supporting records (for example gifts and hospitality logs, conflict of interest logs, expense records, training completion rates) to check that the relevant policies are working in practice.
- Review training records regarding AB & AT training provided to employees and sales and commercial intermediaries and when the last trainings were provided.
- For a sample of employees, verify that trainings have been attended during the in-scope audit period.

2.5 ISSUE MANAGEMENT & INVESTIGATION

10. Procedures shall be implemented to encourage people to report in good faith (suspects) of breaches regarding bribery & anti-trust law. This shall allow anonymous reporting and ensure protection from retaliation. Procedures shall also detail out the required assessment or investigation of any breaches, and appropriate actions to be taken.

What to test

- That a procedure to report any breaches regarding AB & AT is in place.
- That there is a clear stance regarding non-retaliation and the possibility for employees to report anonymously.

- That the speak-up process is known and understood in the company and concerns are reported.
- That suspected bribery cases or breaches of anti-trust legislation have been thoroughly investigated and appropriate steps taken to mitigate the risk of recurrence.
- That the organization monitors and reviews the effectiveness of its reporting and investigation procedures, and issues investigated are used to enforce the CMS.

How to test

- Interview the *compliance officer (or equivalent)* or responsible employee for the process to understand how it operates, how it has been promoted, and its usage for reporting AB & AT concerns.
- Interview a selection of *employees* to assess their awareness of the speak-up process and understanding of its purpose and usage.
- Verify that there is a Whistleblower Policy (or equivalent) that includes a stance on non-retaliation and an investigation protocol.
- Review communications provided about the speak-up process.
- Assess the reporting line and verify that anonymous reporting is possible.
- Review monitoring and evaluation reports to confirm that reporting and investigation procedures are regularly assessed and used to enforce the CMS.

2.6 MONITORING & TESTING

11. The organisation shall implement financial (related to treasury, segregation of duties, expenses, etc.) and non-financial internal controls (related to procurement, sales, pricing, human resources, etc.) to mitigate the risks detected through an enterprise or compliance risk assessment on an organisational or transactional level. The methodology applied by the applicant/member shall be documented and in line with recognized standards.

What to test

- That an internal control framework is established and documented, covering key financial and non-financial risks.

How to test

- Interview the *risk manager (or equivalent)* or *compliance officer (or equivalent)* to understand the internal control methodology and how the relevant controls are monitored.
- Review that the internal control charter or methodology is documented, and key financial and non-financial risk areas are covered through internal controls in line with international practices (e.g. ISO31000, COSO).
- Review evidence of design and implementation of key financial and non-financial controls.

12. Internal audits shall be conducted in the context of the CMS and include AB & AT risks. Aside, the compliance function shall regularly review the CMS to ensure its effectivity for the organization and take actions ensuring continuous improvement.

What to test

- That the compliance function documents a review of its CMS on a regular basis.
- That the organization has mechanisms for continually improving the CMS based on internal audits, compliance reviews and lessons learned.
- That the internal audit plan includes a review of the CMS and relevant AB & AT risks.
- That the compliance function conducts monitoring and oversight in conformity with AB & AT requirements.

How to test

- Interview the *risk manager (or equivalent) or compliance officer (or equivalent)* to understand the internal control methodology and how the relevant controls are monitored.
- Interview the *chief audit executive (or equivalent)* and understand the role of internal audit in reviewing AB & AT risks, and the CMS in general.
- Interview the *compliance officer (or equivalent)* to understand how monitoring and oversight conformity with AB & AT requirements is performed and to assess how the CMS is reviewed on a continuous basis.
- Review the audit plan covering the period in scope and verify that AB & AT topics are explicitly included. Obtain the internal audit report of the respective audit to review recommendations and verify how feedback from (internal) audits (e.g., findings, recommendations) has been integrated into the organization's broader compliance and risk management strategies.
- Review the CMS improvement plan or records to confirm that continual improvement processes are in place. Check for evidence of implemented improvements (e.g., updated policies, enhanced processes).
- Review evidence of the latest CMS review performed by the compliance officer and which updates were made on trends and insights.

3 RISK ASSESSMENT

3.1 RISK ASSESSMENT ON SALES AND COMMERCIAL INTERMEDIARIES

This section focuses on sales and commercial intermediaries, as they might pose an increased risk regarding bribery & anti-trust law since they act as a bridge between the member/applicant and the customer. Types of sales and commercial intermediaries considered in scope are: sales agents, distributors, resellers, sales consultants, and sales advisors (refer to Annex 5.1 for the definitions). A specific risk assessment shall be conducted on sales and commercial intermediaries that are leveraged by the organisation to conduct its business.

Risk assessments shall be conducted on an individual level¹⁴ and shall consider at least the criteria in Section 3.1.1. Where relevant, the organisation shall consider additional, specific risk criteria. The risk assessment should be reviewed at least every two years, or if required by material changes in contractual agreement such as changes in remuneration, payment, or activity region.

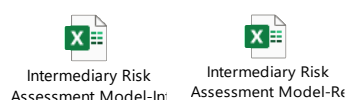
Service partners (defined in the Annex 5.1) are not required to undergo a risk assessment where they are being paid at market rates, but mitigation measures should be applied as appropriate.

3.1.1 Criteria

The following criteria must be considered when conducting a risk assessment and will form the basis of scoring compliance with the standard. Members may choose to assess additional criteria for their own purposes, but the ranges and weights per category should be equal to or stricter than the ones stipulated in the *risk assessment template*. An accurate distinction shall be made between sales and commercial intermediaries, and resellers and distributors.

- Corruption Perception Index (CPI) of the country as published by Transparency International in which the intermediary operates to represent or support the member/applicant, based on the CPI score at the time the risk assessment is conducted. Where the intermediary operates in more than one country, the CPI of the highest risk country will be used;
- Type of sales and commercial intermediary per contractual agreement as defined in the risk assessment model;
- Remuneration model as defined in the risk assessment model;
- Potential remuneration per year and remuneration as percentage of customer contract value (sales agents, sales consultants and sales advisors only); and
- Total percentage for product/per year (resellers and distributors only).

3.1.2 Intermediary Risk Assessment Models



¹⁴ Referring to the level of the natural or legal person. In case the sales and commercial intermediary has multiple contracts, regions etc., the highest risk criteria should be applied.

What to Test

- That the risk assessment is executed and documented for all sales & commercial intermediaries on an individual level.
- That each risk assessment includes at least the above risk criteria, and the assessment has been accurately made.
- That the risk assessments are reviewed at least every two years or sooner if required by material changes in contractual agreement as changes in remuneration, payment, or activity region.

How To Test

- Interview the *compliance officer (or equivalent)* to understand how the relevant population of sales and commercial intermediaries are identified, the risk assessments are executed and documented, and any material changes are flagged that lead to a risk assessment update.
- Confirm the existence of a documented risk assessment for the population of sales and commercial intermediaries.
- Verify that the assessment has been updated at least every two years.
- If applicable, assess the relevance of additional criteria used for the risk assessment.
- For a random sample:
 - Confirm that they are adequately classified between low, medium, or high risks leveraging supporting documentation. The classification should be adequate for each criterion and the total risk score.

3.1.3 Mitigation measures

What to Test

- That the relevant mitigation measures are implemented (with the minimum measures listed in section 3.1.3.1. and following), depending on the risk assessment outcome to reduce the risk exposure to the appropriate level.

How To Test

- Interview the *compliance officer (or equivalent)* to assess how mitigation measures are applied for sales & commercial intermediaries.
- Interview the *sales director (or equivalent)* to understand the involvement of the sales employees in the risk assessment and implementation of mitigation measures.
- For a sample of sales and commercial intermediaries, in accordance with the sampling guide, the assessor will review that the required mitigations in Sections 3.1.3.1 to 3.1.3.6 based on the risk level of the intermediary determined by the risk assessment are completed by the applicant/member.

3.1.3.1 Due diligence questionnaire & screening

Mitigation measure	Low Risk	Medium Risk	High Risk
Internal & External Due Diligence questionnaires	Completed by internal sales organisation and sales and commercial	Completed by internal sales organisation and sales and commercial	Completed by internal sales organisation and sales and commercial intermediary before contracting.

	intermediary before contracting ¹⁵ .	intermediary before contracting.	
Due Diligence screening¹⁶	Internal due diligence screening ¹⁷ before contracting and at least each three years.	Internal due diligence screening before contracting and at least each three years.	External due diligence by an acknowledged audit or investigation company or a due diligence provider before contracting and each three years.

3.1.3.2 Contract approval

Mitigation measure	Low Risk	Medium Risk	High Risk
Contractual agreements for all sales and commercial intermediaries	Contractual agreements should stipulate clear and detailed scope of work (product/project, region, duration, estimated timeframe) including basis for remuneration.	Contractual agreements should stipulate clear and detailed scope of work (product/project, region, duration, estimated timeframe) including basis for remuneration.	Contractual agreements should stipulate clear and detailed scope of work (product/project, region, duration, estimated timeframe) including basis for remuneration. Remuneration should be based on a documented reasoning ¹⁸ .
Resellers and Distributors contracts	Contractual provisions stipulating: - that products cannot be sold, resold or distributed in sanctioned territories	Contractual provisions stipulating: - in what territories the products can be resold and prohibitions on	Contractual provisions stipulating: - in what territories the products can be resold and prohibitions on redirection to sanctioned countries

¹⁵ Data that should at least be requested in the external questionnaire: contact details, company details (office address, registration in commercial register, DUNS number, incorporation documents), region where work is being performed, timeframe for the work, shareholders/UBOs, representatives, declaration of legal proceedings, intended service, names of subcontractors (if any), bank letter & account details, business references.

Data that should at least be requested in the internal questionnaire: new/existing relationship, type of intermediary, CPI for registered office & location of activity, online research, knowledge of past incidents, in scope activities, remuneration type and support.

¹⁶ At a minimum, due diligence shall include: (1) Adverse Media (including checks relating to ABC, Antitrust/Competition, Fraud, Financial Crime, Organised Crime, Tax Crime); (2) PEP listings, including family members and close associates checks (current); (3) Sanctions listings, including any listings on UK, US, EU and UN sanctions lists and any other official lists; (4) Financial strength indicators; and (5) checks related to any red flags that arise from the external questionnaire. If any of these cannot be checked and reviewed, then the member shall document the reason why they could not be completed and shall perform alternative/additional due diligence to assess based on what is reasonable in the circumstances.

¹⁷ Screening should be done by using information such as adverse media provided by an acknowledged source (database, country report, etc.)

¹⁸ The documented reasoning should justify the type and amount of remuneration (e.g. linked to legal entity structure, estimate of effort spent translated to FTE, benchmark with remuneration of senior professionals for that region, etc.)

	and prohibiting redirection to sanctioned countries - when the reseller/distributor asks for additional discounts/margins from the member in order to secure a customer, the contract must state this special pricing must be passed through to the end customer	redirection to sanctioned countries - when the reseller/distributor asks for additional discounts/margins from the member in order to secure a customer, the contract must state this special pricing must be passed through to the end customer	- when the reseller/distributor asks for additional discounts/margins from the member in order to secure a customer, the contract must state this special pricing must be passed through to the end customer
Approval of the contract by Senior Management or delegates	Approval needed by Senior Management or appointed delegates before signing the contract.	Approval needed by Senior Management or appointed delegates before signing the contract.	Approval needed by Senior Management before signing the contract.

3.1.3.3 Awareness & monitoring

Mitigation measure	Low Risk	Medium Risk	High Risk
Activity reports	Activity reports to be submitted at least on a quarterly basis for the duration of the contract, and reviewed and approved by sales department on content and quality ¹⁹ .	Activity reports to be submitted at least on a quarterly basis for the duration of the contract, and reviewed and approved by sales department on content and quality.	Activity reports to be submitted at least on a quarterly basis for the duration of the contract, and reviewed and approved by sales department on content and quality.
Compliance confirmation²⁰	Compliance confirmation every three years.	Compliance confirmation every two years.	Annual compliance confirmation.
Training	eLearning or via other platform (at minimum) at the start of contractual term and every three years.	eLearning or via other platform (at minimum) at the start of contractual term and every two years.	eLearning or via other platform (at minimum) at the start of contractual term and every two years.

¹⁹ The quality of the activity report can be assessed according to the degree of granularity or details. It relates to the quality of information provided by the intermediary. The content can be evaluated based on concrete actions carried out in compliance with the contract and company policies. For resellers and distributors, activity reports should include sales activity information which allows for the company and the assessor to determine there has been no corruption or bribery, but which does not violate AT laws in the applicable territories.

²⁰ Following the compliance confirmation, sales and commercial intermediaries confirm they comply with national and international laws where applicable and they have read and understood company's policies and procedures. The compliance confirmation needs to be reconfirmed periodically. It's a separate document from any contract prerequisite and it can't be considered as a one-time action.

3.1.3.4 Payment approval

Mitigation measure	Low Risk	Medium Risk	High Risk
Resellers and Distributors Pricing	Justification for special pricing granted to resellers and distributors that deviates from company standard must be provided by intermediary and sales department before approval given	Justification for special pricing granted to resellers and distributors that deviates from company standard must be provided by intermediary and sales department before approval given	Justification for special pricing granted to resellers and distributors that deviates from company standard must be provided by intermediary and sales department before approval given
Remuneration over threshold amount²¹	--	Actual and potential remuneration over USD\$400,000/5% will receive approval from the CEO (or equivalent or general counsel), CFO and compliance officer as per the Board's delegation of authority.	Actual and potential remuneration over USD\$400,000/5% will receive approval from the CEO (or equivalent or general counsel), CFO and compliance officer as per the Board's delegation of authority.
Approval of deviating payment	Approval by Senior Management or a delegate committee of a payment deviating from the contractual agreed payment scheme is required even if the threshold amounts are not exceeded.	Approval by Senior Management or a delegate committee of a payment deviating from the contractual agreed payment scheme is required even if the threshold amounts are not exceeded.	Approval by Senior Management or a delegate committee of a payment deviating from the contractual agreed scheme is required even if the threshold amounts are not exceeded. In that case, the approval should be done based on a compliance statement or after a review of compliance. ²²

²¹ The threshold amount is greater than \$400,000 per year or greater than 5% of the customer contract value. Approval will be obtained prior to signing the initial contract and prior to any amendments that would increase, or further increase, the contract amount over the threshold amounts. It is not possible to be low risk when paying over the remuneration thresholds.

²² The compliance function should be involved in the approval process and it should be documented. The compliance function can either do a case-by-case file review per payment, or submit a statement on intermediary level that mitigation measures were taken.

3.1.3.5 Remuneration over Threshold Amounts²³

Mitigation measure	Low Risk	Medium Risk	High Risk
Risk Assessment Sign Off	Not possible to be in this category	Signoff of risk assessment by compliance, CFO and CEO	Signoff of risk assessment by compliance, CFO and CEO
External Due Diligence	-	External due diligence ²⁴ by qualified third party	External due diligence ²⁵ by qualified third party
Contract Approval	-	Written contract approval by CEO and compliance function	Written contract approval by CEO and compliance function
Additional Mitigations	-	One or more of: (a) Contract provision on right to perform an external audit if reasonable suspicion of corruption (b) Contract provisions on payments put in trust where there is an official charge or legal allegation	Interview between the assessor and sales and commercial intermediary when the member is undergoing the BnEI audit. ²⁶ One or more of: (a) Contract provision on right to perform an external audit (b) Contract provisions on payments put in trust where there is an official charge or legal allegation

3.1.3.6 Overview of High Risk Intermediaries and Intermediaries over the Remuneration Threshold

For all sales and commercial intermediaries with a high risk grade or intermediaries whose remuneration exceeds \$400,000 in a given year or 5% of the customer contract value in the aggregate, an overview will be compiled by the compliance function which will be shared with the assessors and the Accreditation Council to create transparency on the respective mitigation measures. The overview will contain a breakdown of the sales and commercial intermediary's remuneration and reimbursed expenses. A sample of supporting activity reports, as selected by the assessor, will be provided. The applicant/member will provide justification for the remuneration of the sales and commercial intermediaries.

²³ The threshold amount is greater than \$400,000 per year or greater than 5% of the customer contract value.

²⁴ The member will perform and/or review, at minimum, the due diligence requirements stated in Section 3.1.3.1 above, to the extent possible, and other relevant factors, such as criminal record check; educational and professional verification; corporate registrations; litigation records or media findings; and professional sanctions.

²⁵ The due diligence requirements under medium risk will be completed. Further, a suitably independent individual, either internal compliance or external, to conduct an oral interview with the intermediary. The interview will be documented.

²⁶ If a member does not have any sales and commercial intermediaries who are in this risk category, then the assessor shall interview a sample of the member's sales and commercial intermediaries in other risk categories.

3.2 CHECK LIST – HIRING FORMER GOVERNMENT OFFICIAL OR PEP

Specific mitigation measures shall be applied if the applicant/member would recruit former government officials and/or Politically Exposed Persons ('PEP') who will interact with government officials. As a result, the following checklist needs to be leveraged in the recruitment process prior to contracting a new employee. If the former government official or PEP is retained as a sales and commercial intermediary (e.g. not a full-time employee), then the requirements of 3.1 are required in addition to the requirements included in 3.2.

3.2.1 Risk criteria

- Based on screening results and/or complementary information, the candidate is confirmed to be a former government official or PEP (including family members or close associates). (yes/no) (1 p.)
- The candidate was a Senior Government Employee. (yes/no) (1 p.)
The candidate, in its capacity as a PEP or Senior Government Employee, during the three years preceding the employment or contract by the member/applicant was involved or was responsible for the tendering process and/or contract management between the government entity causing the Senior Government Employee or PEP designation and the applicant/member. (yes/no) (1 p.)

For each positive response (reply 'yes') to the scenarios above, 1 point is awarded to the risk profile of the individual.

What to test

- That a risk assessment is executed and documented on an individual level prior to hiring or contracting a former government official or PEP.
- That the risk assessment of the former government official or PEP includes at least the above risk criteria, and the assessment is accurately made.

How to test

- Interview the *compliance officer (or equivalent)* to understand how the relevant population of former government officials and PEPs are identified, the risk assessments are executed and documented.
- Interview the *human resources director* to understand their involvement in the risk assessment during the recruitment process.
- For the population of former government officials and PEPs:
 - Confirm the existence of a documented risk assessment.
 - If applicable, assess the relevance of additional criteria used for the risk assessment.
 - For former government officials or PEPs that are hired as a consultant, the requirements of Section 3.1 are applied.

3.2.2 Mitigating measures

In case of a score of 1 or above, the applicant/member shall at least apply the following mitigation measures before contracting:

- Review the contractual obligations of the member/applicant to clarify whether any grace period shall be applied relevant to the current employment. If feasible, ask for, review and understand the ethics opinion provided to a former government employee/PEP upon his/her departure from government service/previous employer.

In case of a score of 2, the following principle shall be respected during term of employment:

- Ensure that no employee engages directly with or negotiates on behalf of the company with their former government agency without prior consultation with the member/applicant's compliance function. Additionally, either (i) all such interactions must be documented through comprehensive meeting minutes, or (ii) the employee should be accompanied by a second company representative in all engagements with the former agency.

What to test

- That the relevant mitigation measures are implemented depending on the risk assessment outcome to reduce the risk exposure to the appropriate level.

How to test

- For former government officials or PEPs that are hired as a consultant, the requirements of Section 3.1 are applied.
- Interview the *compliance officer (or equivalent)* to understand how mitigation measures are applied when hiring a former government official or PEP.
- For a sample of hired former government officials or PEPs with a score of 1 or above:
 - Confirm that they are adequately classified leveraging supporting documentation. The classification should be adequate for each criterion and the total risk score.
 - Review the hiring report and confirm at least the following elements are checked before contracting:
 1. The grace period to be applied, if any.
 2. A review of the ethics opinion provided upon their departure from government service/previous employer. If not applicable, ensure there is a documented justification.
- For a sample of hired former government officials or PEPs with a score of 2, verify whether this employee engaged directly with or negotiated on behalf of the company. If this has been the case, verify that:
 1. Prior consultation with the compliance function is documented;
 2. Meeting minutes of all interactions are documented; or
 3. Evidence is available that a second company representative who is not a former government official or PEP joined the conversations.

4 MINIMUM STANDARDS

The following 34 minimum standards shall be applied to all applicants/members in the context of mitigating the risks linked to anti-bribery & anti-trust ('AB & AT'):

4.1 COMMITMENT FROM SENIOR MANAGEMENT (#4)

What To Test 1

- a. The annual compliance program is approved by the governing committee.

How To Test 1

- Verify there is formal approval of the compliance program by the governing committee either via meeting minutes or via a signed compliance program.

What To Test 2

- b. Documented reporting regarding compliance should be done on a half-year basis or after any significant change to the appropriate governing committee.

How To Test 2

- Interview (a) *member(s) of the governing committee* to ascertain how often compliance topics, including the compliance program, are discussed at meetings.
- Verify based on meeting minutes that compliance topics have been discussed at least half-yearly with the governing committee.

What To Test 3

- c. Documented reporting regarding compliance should be done on a quarterly basis or after any significant change to Senior Management.

How To Test 3

- Interview (a) *member(s) of senior management* to ascertain how often compliance topics, including the compliance program, are discussed at meetings.
- Verify based on meeting minutes that compliance topics have been discussed half-yearly with the governing committee, and quarterly with senior management.

What To Test 4

- d. Ongoing compliance communication:
 - a. External communication leveraging the company website with key statements regarding compliance.
 - b. Internal communication: At least 2 messages from Senior Management per year.

How To Test 4

- Interview other *key managers* to verify how messages from senior management have been personally championed.
- Interview a sample of relevant *employees* to verify the effectiveness of the communication on senior management commitment. Verify that the AB & AT policies are published on the company website.
- Review statements and presentations made by senior management to check on the clarity of AB & AT messages.
- Verify that communication related to AB & AT is launched at least two times per year.

4.2 COMPLIANCE POLICIES AND PROCEDURES (#8)What To Test 1

- a. A dedicated compliance officer is appointed with reporting lines to a member of the senior management, without commercial responsibilities, and with access to the governing committee. In cases where, due to the company's size, the compliance officer serves in a shared capacity, they must remain free from any commercial responsibilities.

How To Test 1

- Interview the *compliance officer (or equivalent)* to discuss their remit, workload, reporting lines and any areas of concern they may have regarding resourcing, particularly regarding regional support in high-risk areas.
- Interview the *compliance officer (or equivalent)* to assess whether any conflict of interests occurred and how this is being dealt with.
- Review the compliance officer (or equivalent)'s job description, organization chart and the function's budget.

What to Test 2

- b. Local compliance coverage shall be installed in form of local compliance officers, compliance point of contacts or ambassadors in the organization's hubs or subsidiaries. The member shall establish processes requiring it to investigate suspected AB or AT infringements that come to its attention, carry out a structured internal investigation and, upon obtaining appropriate legal advice, make informed decisions on whether and when to notify relevant government authorities or regulators of such suspected violations.

How To Test 2

- Interview some *local compliance representatives*, if applicable, to assess their awareness with the compliance policies and procedures, and how they ensure compliance at local level.
- Review local presence of the entity and validate that for each hub or subsidiary, a compliance representative is appointed, if applicable.
- Verify that local compliance officers, compliance point of contacts or ambassadors are in contact with the compliance officer (or equivalent) to ensure correct application and understanding of policies, for example via meeting minutes or presentations.

What To Test 3

- c. AB & AT policies are reviewed at least every 3 years.

How To Test 3

- Interview the *compliance officer (or equivalent)* to understand how and by whom policies are periodically reviewed.
- Review that evidence exists of the latest review cycle for all relevant policies and this is less than three years ago.
- Review document control procedures to confirm they include version control, access restrictions, and update mechanisms.

What To Test 4

- d. AB & AT policies shall be communicated to all employees in the organization in a language they understand.

How To Test 4

- Interview the *compliance officer or responsible department manager* to confirm that AB & AT policies are in a language that relevant employees understand.

What To Test 5

- e. AB & AT policies shall at least cover anti-bribery, anti-trust, gifts, hospitality & travel, sponsorships, donations, whistleblowing, forced labor, facilitation payments, political contributions, conflict of interest and dealing with competitors, government officials or sales and commercial intermediaries.

How To Test 5

- Review that policies exist for the following themes: anti-bribery, anti-trust, gifts, hospitality & travel, sponsorships, donations, whistleblowing, forced labor, facilitation payments, political contributions, conflict of interest and dealing with competitors, government officials or sales and commercial intermediaries.

What to Test 6

- f. The AT policy shall contain at least the following elements:
- a. checklists setting out dos & don'ts when interacting with competitors.
 - b. a requirement that a declaration be signed prior to discussions with competitors, where deemed necessary (e.g., in the context of trade associations).
 - c. requirements for third-party presence (e.g., external legal counsel) in respect of high-risk competitor engagements.

How To Test 6

- Review that the AT policy contains at least the following elements:
 - a. checklists setting out dos & don'ts when interacting with competitors.
 - b. a requirement that a declaration be signed prior to discussions with competitors, where deemed necessary (e.g., in the context of trade associations).
 - c. requirements for third-party presence (e.g., external legal counsel) in respect of high-risk competitor engagements.
- For a sample of competitor engagements for which compliance declarations would be required under the AT policy, verify that such declarations were duly signed.
- For a sample of high-risk competitor engagements, verify that the third-party presence requirement was complied with.

What to Test 7

- g. Extended Management team (based on company definition) and commercial teams shall acknowledge in writing their personal compliance with the AB & AT policies on an annual basis.

How to Test 7

- Interview some *members of the extended management team and commercial team* and assess their awareness with the compliance requirements and AB & AT policies.
- For a sample of members of the extended management and commercial teams, verify if the Annual Compliance Conformity Declaration is signed for one of the years in-scope of the audit period.

What to Test 8

- h. An approval process shall be established that runs through the compliance function to approve non-trivial gifts, hospitality and travel for government officials, current customers and prospective customers, or received by member employees in the context of their professional activity. The compliance function shall ensure all non-trivial gifts and hospitality are properly recorded and maintained, whether provided to an official, customer or received by a member employee.

How To Test 8

- Interview the compliance officer (or equivalent) to ascertain how employees and sales and commercial intermediaries are required to receive approval and report gifts and hospitality offered.
- Review the records for non-trivial gifts, hospitality and travel exist.
- Interview relevant *employees* to verify their understanding of the relevant procedures.
- For a sample of employees, validate that records of non-trivial gifts, hospitality and travel are properly recorded, maintained and approved.

4.3 RISK ASSESSMENT (#4)What to Test 1

- a. A risk assessment shall be executed that explicitly covers AB & AT topics.

How To Test 1

- Interview the *risk manager (or equivalent)* or *compliance officer (or equivalent)* to assess the processes for identifying and monitoring bribery and anti-trust risks and controls.
- Interview the *risk manager (or equivalent)* or *compliance officer (or equivalent)* to understand how relevant interactions with competitors are identified for AT risks.
- Verify that the risk assessment is well documented and includes relevant bribery and anti-trust risks and controls.

What to Test 2

- b. The risk assessment shall be updated every two years. In the event there is a material change to the member organization, the risk assessment shall be updated immediately.

How To Test 2

- Verify that there is evidence of review of the risk assessment in the past two years, or in case of a material change.

What to Test 3

- c. The risk assessment shall be acknowledged by the Senior Management and governing committee.

How To Test 3

- Verify that there is evidence of review of the risk assessment in the past two years, or in case of a material change.
- Acknowledgement of senior management is documented via sign-off or meeting minutes.

What to Test 4

- d. Members shall have procedures in place to manage AB & AT risks in the context of mergers, acquisitions, joint ventures and other forms of business collaborations, including for carrying out due diligence. If the other organization is a BnEI member, further AB due diligence is not required.

How To Test 4

- Review the procedure for conducting due diligences for mergers, acquisitions, joint ventures or other forms of business collaboration and verify that this procedure also contains rules to manage AB & AT risks.
- For a sample of past mergers, acquisitions, joint ventures or other business collaboration occurring within the previous three year period, verify that due diligence procedures (including AB & AT aspects) were fully respected.

4.4 TRAINING AND CONTINUING ADVICE (#6)

What To Test 1

- a. A defined training strategy and approach shall be documented.

How To Test 1

- Interview the *compliance officer (or equivalent)* to understand how employees are being trained and made aware of the AB & AT requirements, and how this is specified depending on the risk profile of the employee.
- Review the documented training strategy and approach.

What To Test 2

- b. Training shall cover, at a minimum, the company's AB & AT policies.

How To Test 2

- Verify that AB & AT topics have been included in the training.

What To Test 3

- c. A target audience analysis shall be performed to determine who should be trained and on what subjects.

How To Test 3

- Interview a selection of *other employees* and verify whether they have read and understood the content of the policies, and whether they received the appropriate AB & AT training depending on their risk profile.
- Review whether employees follow different types of training depending on their risk profile, and in the appropriate language (to cover at least 80% of the target population) and how this assessment has been made.

What To Test 4

- d. Interactive training shall be conducted for relevant and high risk or control employees and other high risk functions for a duration of at least two hours in three years (frequency can be adapted to the context, being it face-to-face or virtual trainings).

How To Test 4

- Review the content for the interactive training and the eLearning to cover the proper timing range.
- For a sample of employees, validate the assessment (higher risk) and confirm that they followed the appropriate AB & AT training.

What to Test 5

- e. eLearning shall be conducted for the lower risk group at least every two years with an updated training content with at least 20 minutes for AB & AT. Those virtual learnings must be translated, as required, to cover the company's target population (based on the target audience analysis, see "c" point above). If no eLearning platform is available, other training channels (e.g. classroom) can be leveraged.

How To Test 5

- Review the content for the interactive training and the eLearning to cover the proper timing range.
- For a sample of employees, validate the assessment (lower risk employees) and confirm that they followed the appropriate AB & AT training.

What to Test 6

- f. Performance evaluations shall take into consideration completion of compliance training.

How To Test 6

- For a sample of employees, validate that the completion of compliance trainings was part of their last performance evaluation.

4.5 THIRD PARTY MANAGEMENT (#6)

For the required mitigation measures per sales and commercial intermediary, we refer to section 3.1 Risk Assessment. Compliance shall perform, at minimum, the following controls on all sales and commercial intermediaries.

What to Test 1

- a. Internal and external questionnaires shall be reviewed by compliance before contracting.

How To Test 1

- Interview the *compliance officer (or equivalent)* and assess that the compliance monitoring activities have been performed in a consistent manner and understand the process for periodic review of compliance policies and procedures.
- For a sample of internal and external questionnaires, verify that formal review was performed by compliance before contracting.

What to Test 2

- b. Compliance should conduct regular spot checks on the quality of activity reports to ensure accuracy, completeness, and adherence to regulatory requirements. These checks must be documented, and any discrepancies or issues should be promptly addressed and reported to Senior Management.

How To Test 2

- Review the control performed on quality of activity reports and verify that these have been documented, and actions have been taken in case of non-compliance.

What to Test 3

c. Compliance should follow-up on completion rates of trainings.

How To Test 3

- Review the control performed on completion rates of training and verify that these have been documented and actions have been taken in case of non-compliance.
- For a sample of sales and commercial intermediaries, verify that training has been provided and completed.

What to Test 4

d. Compliance should follow-up on completion rates of declarations of compliance with policies and procedures.

How To Test 4

- Review the control performed on completion rates of compliance declarations and verify which actions have been taken in case of non-compliance.

What to Test 5

e. Compliance shall ensure there are AB and AT provisions in intermediary contracts, including adherence to company AB and AT policies, and penalties for AB or AT violations up to and including termination of the contract. Compliance or Legal (internal or external) shall approve the intermediary contract prior to signature.

How To Test 5

- For a sample of intermediary contracts, verify that formal approval was given by compliance before sign-off and they contain AB & AT provisions.

What to Test 6

f. Compliance shall maintain a register of intermediaries who interact with government officials on the company's behalf.

How To Test 6

- Review that there is a register of intermediaries who interact with government officials.

4.6 CONFIDENTIAL REPORTING, INTERNAL INVESTIGATION AND DISCIPLINARY MEASURES (#4)

What to Test 1

a. The company shall have clear disciplinary procedures in place and enforce them consistently across the organization, which such procedures will include appropriate and documented disciplinary action for non-compliance with the company's AB & AT policies.

How to Test

- Review the procedure to investigate and report any AB & AT infringements by employees or sales and commercial intermediaries.
- For a sample of employees, review contractual clauses on AB & AT policies and disciplinary action, including termination rights.

What To Test 2

- b. The company shall have an efficient and trusted mechanism by which employees and third parties can anonymously or confidentially report allegations of a breach of the company's code of conduct, company policies, or suspected or actual misconduct.

How to Test 2

- Interview the *compliance officer (or equivalent)* or responsible employee for the process to understand how it operates, how it has been promoted, and its usage for reporting AB & AT concerns.
- Interview *employees* to understand awareness on, and the level of trust towards, the speak-up mechanism.

What To Test 3

- c. The company shall have a complaint-handling process with clear roles & responsibilities, complaint handling protocol to ensure timely and confidential treatment of complaints. Analysis shall be done to improve company policies & procedures where needed.

How to Test 3

- Interview the *compliance officer (or equivalent)* and verify how reports and complaints are used to improve the CMS.
- Review the procedure for complaint handling and verify whether this ensures timely and confidential treatment of reports.

What To Test 4

- d. Compliance shall have access to relevant reporting & investigative information needed to perform the root-cause analysis.

How to Test 4

- Review the access of the compliance function to relevant files and information.

4.7 CONTINUOUS IMPROVEMENT AND REVIEW (#2)

What To Test 1

- a. A set of at least 11 financial and non-financial internal controls shall be established to evidence effectiveness, based on the organization's context. If applicable, the following minimum internal controls shall be designed and implemented:
 - a. require segregation of duties on price approvals, including discounts, credit terms and sales incentives, for customer contracts

-
- b. require at least two persons to evaluate tenders and award contracts
 - c. implement a four-eyes review for initiating and approving banking payments (including petty cash)
 - d. implement different levels of authority for approval of expenditures and disbursements
 - e. implement a three-way match on goods/service receipt
 - f. conduct periodic bank account reconciliations
 - g. install a periodic review and approval process of accruals
 - h. perform four-eyes validation of beneficiary bank details (creation/modification)
 - i. implement limitations on access rights to confidential information
 - j. periodic review of compliance policies and procedures
 - k. payments made only through recorded bank transfers to the third party's approved account

This list should not be exhaustive.

How To Test 1

- Interview the *sales director (or equivalent)* to understand the design and implementation of segregation of duties on price approvals, discounts, credit terms, and sales incentives; and, to understand the approval process for tenders and contract awards.
- Interview the *finance manager (or equivalent), treasury officer (or equivalent), controller (or equivalent) or accountant (or equivalent)* to discuss the implementation of a four-eyes review for creating or modifying beneficiary bank details and making banking payments, process for periodic bank account reconciliations, enforcement of authority levels for expenditures and disbursements, process for review and approval of accruals, confirm proper controls over financial transactions, and understand how it can be ensured that payments are made only through recorded bank transfers to approved third-party accounts.
- Interview the *procurement manager (or equivalent) or the warehouse manager (or equivalent)* to ensure the three-way match process is in place for goods and service receipts.
- Interview the *IT manager (or equivalent)* to assess limitations on access rights to confidential information.
- Review the internal control framework and verify that at least the minimum controls are established and monitored.
- Review evidence of design and implementation of key financial and non-financial controls.

What to Test 2

- b. There are appropriate internal audits which include AB and AT checks.

How To test 2

- Interview the *risk manager (or equivalent) or compliance officer (or equivalent)* to understand the internal control methodology and how the relevant controls are monitored.
- Interview the *chief audit executive (or equivalent)* and understand the role of internal audit in reviewing AB & AT risks, Compliance culture, and the CMS in general.
- Review the audit plan covering the period in scope and verify that AB & AT topics are explicitly included.

- Obtain the internal audit report of the respective audit to review recommendations and verify how feedback from (internal) audits (e.g., findings, recommendations) has been integrated into the organization's broader compliance and risk management strategies.
- Review the CMS improvement plan or records to confirm that continual improvement processes are in place. Check for evidence of implemented improvements (updated policies, enhanced processes).

5 ANNEXES

5.1 DEFINITIONS

- **Senior Management:** group of executives and leaders, including the executive management team, who are responsible for both strategic decision-making and operational oversight. This group typically includes the highest executive leadership within the organization.
- **Governing Committee:** Board of Directors or a group of individuals authorized by the Board of Directors, consisting of non-executives and independent directors, ultimately responsible for overseeing the company's strategic direction, decision-making, and governance processes.
- **Delegate committee:** person or group of people who are authorized to act on behalf of the executive committee in the context of a specific domain or decisions. The delegate committee operates under clear guidelines and is entrusted with defined responsibilities (e.g. in Delegation of Authority). They are accountable to the Senior Management and the Governing Committee for the outcomes of their tasks.
- **Applicant:** organization seeking accreditation from the Banknote and Ethics Initiative. Applicants must pass an AB & AT audit to get accredited.
- **Member:** organization which is accredited by the Banknote and Ethics Initiative.
- **Employees:** company's director, officers, staff, or workers, and volunteers. The term employee covers both permanent payroll employees and named individuals employed on fixed-term contracts either with the applicant/member directly or via a sales and commercial intermediary agency. It does not cover persons who are working in the company as part of third-party service contract via a service provider.
- **Third parties:** independent external party with whom company has, or plans to establish, some form of business relationship. These could include companies that provide specialized services like security features, logistics, customer engagement, etc.
- **Sales and commercial intermediaries:** third parties that act as a bridge between the banknote company and the end customer, facilitating transactions, negotiations, or logistics. They're often involved in managing communication, contracts, sales process, etc. Those include sales agents, distributors, resellers, sales consultants, sales advisors, or service partners.
- **Sales agents:** individual or entity acting on the company's behalf in negotiating and securing sales. Sales agents have direct influence over sales and client relationships. Typically remunerated on a commission base, success fee or retainer base.
- **Sales advisors:** individual or entities providing strategic advice to the company, but have no customer involvement unless the company is present.
- **Distributors:** third-party entities or individuals that purchases banknotes or related products from the manufacturer and resells them to retailers, end customers, or other businesses with a designated territory. Distributors take ownership of the product and are responsible for the flow of goods in specific regions, often involving high-value transactions and complex logistics. These entities are typically remunerated on a margin base.
- **Resellers:** entity or individual that purchases banknotes or related products from manufacturers or distributors and resells them to other clients, often without a specific territorial agreement. Resellers operate in secondary markets, which can be more difficult to monitor and regulate. Typically remunerated on a commission base, success fee or retainer base.
- **Sales consultant:** expert such as a lobbyist or facilitator providing specialized advice and strategy in relation to sales, market entry, and customer acquisition. They are typically involved in the direct sale or handling of products. Typically remunerated on a commission base, success fee or retainer base.

-
- **Service Partner:** Organizations or individuals who partner with a company to offer services related to the company's products. They may provide legal, logistics, customs, installation, maintenance, training, or support services.
 - **Politically Exposed Persons (PEPs):** an individual who holds, or has held, a prominent public position, domestically or internationally, which could expose the member to potential AB & AT risks. PEPs include government officials, senior government employees, military leaders, judges, central bank executives, or other individuals with substantial public authority that may have influence over financial system, regulations and management of currency. It also applies to family members or close associates of such persons.
 - **Government official:** these include people who hold a legislative, administrative or judicial office (either appointed or elected) or any person exercising a public/government function, including for a public agency or a public enterprise (e.g. a state owned enterprise).
 - **Senior Government Employee:** refers to an individual who holds a senior management or leadership position within the government or a government agency. These individuals often have significant decision-making authority, oversee major programs or departments, and may have a high level of influence within the organization. Roles may include cabinet members, department heads, agency directors, and other top-level officials responsible for shaping and executing government initiatives and strategies.
 - **Stakeholders:** the term 'stakeholders' typically includes the applicant/member company's managers, employees, service provider employees, sales and marketing agents, agents interacting with government officials on the company's behalf (including lobbyist and political consultants), key sub-contractors and joint venture partners. While customers would normally be considered stakeholders of the applicant/member, they are excluded from this definition because of the difficulty of interviewing them in practice.
 - **Corruption Perception Index:** it measures how corrupt each country's public sector is perceived to be, according to experts and businesspeople.
 - **Tendering:** it refers to the pre-contractual process including request for bids, their submission and evaluation, the selection of third parties and finally the contract negotiation and signing.
 - **Family Members:** includes spouses or common-law partners, biological, step or adoptive children, parents, the parents of spouses or common-law partners, and biological and step siblings.
 - **Close Associates:** means a person connected to a PEP for personal or business reasons. Examples of close associates include, but are not limited to, business partners, persons in a romantic relationship with a PEP, and persons involved in financial transactions with a PEP. A person ceases to be considered a close associate when they lose that connection.

5.2 AUDIT SCOPE FORM

BnEI 2.0 | Audit Scope Form

BnEI 2.0 Audit Scope Form	
1.	Please describe the overall structure of your organization (e.g. where the organization's head office is located, if you operate by global regions or country and where the key operational sites and subsidiaries are located).
2.	Please describe your business lines, highlighting any which are not related to the banknote industry ²⁷ .
3.	Is your organization or its regional sites or subsidiaries ISO 37001 accredited or in the process of being accredited?
4.	Where is your senior management and governing committee based and where are the members located?
5.	Did your organization recently (past 3 years) engage in any mergers, acquisitions or joint ventures?
6.	How many employees do you employ in total? How many employees are based at the organization's head office?
7.	Please give a breakdown of the number of employees, sales agents, distributors, resellers, sales consultants, and sales advisors your organization has per regional site/subsidiary, specifying the difference between internal (directly employed by your organization) and external (third-party or independent) roles. (<i>see table</i>)
8.	Please indicate where the following functions are located (at the head office only, mostly at head office or which regional site/subsidiary): operations, finance and accounting, sales, legal & compliance and procurement. (<i>see table</i>)
9.	Has your organization experienced any compliance issues related to anti-bribery and anti-trust in the past three years?

²⁷ Banknote activities include, but are not limited to: sale of banknotes or related products and services such as paper, ink, machinery, and security features; service provisions related to banknote design, production or handling; contracting for banknote-related projects or operations; lobbying within the banknote industry; engineering of banknote production, security features, or related technology; logistics involved in the transportation and secure handling of banknotes or related products.

Question 7. Table

	Internal	External				
Regional site/subsidiary	# employees	# sales agents	# distributors	# resellers	# sales consultants	# sales advisors

Question 8. Table

	At head office only	Mostly at head office	Regional site/subsidiary
Operations			
Finance and Accounting			
Sales			
Legal & Compliance			
Procurement			

5.3 DOCUMENT REQUEST LIST

BnEI 2.0 | Document Request List

Baseline CMS Principles

Depending on whether ISO certification is in place or not, a selection of the documents listed below can be made by the assessor.

Document Name	Status
Documentation describing the approved CMS including evidence of review	
Approved CMS policies, e.g.: <ul style="list-style-type: none"> • Anti-bribery policy • Anti-trust policy • Gifts, hospitality & travel policy • Sponsorships & donations policy • Forced labor policy • Facilitation payments policy • Political contributions policy • Conflict of interest policy • Government officials' policy • Sales and commercial intermediaries' policy 	
Evidence that CMS related policies have been communicated to all business units, governing committees (and customers, if applicable)	
Compliance officer's job description and budget	
Organisation chart (of the organization and compliance function)	
Risk assessment including AB & AT risks and mitigation measures	
Monitoring and evaluation reports regarding risk mitigation measures (past 3 years)	
Monitoring and evaluation reports regarding reporting and investigation procedures (past 3 years)	
Procedure related to gifts, hospitality and travel AB risks and mitigation measures	
Document management system of CMS related policies	
Due diligence procedure for (potential) employees	
Attendance records regarding AB & AT training (past 3 years)	
Remuneration policy	
Evidence of promotion of speak-up culture (e.g. via the intranet, policies, training)	
Whistleblower policy	
Internal control charter or methodology	
Audit plan (past 3 years)	
Internal audit report regarding AB & AT topics	
Procedure for reporting and escalating AB & AT issues	
Overview of past compliance issues (past 3 years)	
CMS improvement plan or records and evidence of review by the compliance function	

Risk Assessment for Banknote Specific Risks

<i>Document Name</i>	<i>Status</i>
Overview of high risk intermediaries and intermediaries over the remuneration threshold	

Minimum Standards

Documents in the list below might overlap with the Baseline CMS Principles document list as it is depending on the audit context which documents will be requested in the latter. The assessor shall perform a check on duplicate requests before sharing this with the applicant/member.

<i>Document Name</i>	<i>Status</i>
Evidence of formal approval of the compliance program	
Meeting minutes with evidence of half-yearly discussion of compliance topics with the governing committee	
Meeting minutes with evidence of quarterly discussion of compliance topics with senior management	
Examples of statements and presentations made by senior management on AB & AT messages	
Approved AB & AT policies, e.g.: <ul style="list-style-type: none"> • anti-bribery policy • anti-trust policy • gifts, hospitality & travel policy • sponsorships & donations policy • Forced labor policy • Facilitation payments policy • Political contributions policy • Conflict of interest policy • Government officials' policy • Sales and commercial intermediaries' policy 	
Evidence that AB & AT policies are published	
Compliance officer (or equivalent)'s job description	
Organisation chart (of the organization and compliance function)	
Compliance budget	
Evidence of communication between local compliance representatives and the compliance officer	
Document management system of AB & AT policies	
Documented risk assessment including AB & AT risks and controls	
Records for non-trivial gifts, hospitality and travel	
Procedures for conducting due diligence for mergers, acquisitions, and joint ventures	
Anti-Trust Checklist for employees	
Training strategy and approach regarding compliance trainings	
Content of interactive trainings	
Content of eLearning	

Evidence of the compliance function performing checks on activity reports and actions in case of non-compliance	
Evidence of follow-up performed by the compliance function on completion rates of trainings	
Evidence of control performed by the compliance function on completion rates of compliance declarations	
Register of intermediaries who interact with government officials	
Investigation procedure to report AB & AT infringements	
Procedure for complaint handling	
Internal control framework	
Evidence of design and implementation of key financial and non-financial control	
Audit plan (past 3 years)	
Internal audit report regarding AB & AT topics	
CMS improvement plan	

Population Files

In phase 1 of the testing during the audit, the assessors request a list of the populations mentioned below over the in-scope audit period. Please find the template overview for sales and commercial intermediaries and resellers and distributors on page 48.

Populations	Status
A list of active sales and commercial intermediaries	
A list of active resellers/distributors	
A list of high-risk function employees	
A list of employees	
A list of sales employees	
A list of hired former government officials or PEPs	
A list of interactions/contracts with competitors (past 3 years)	
A list of mergers, acquisitions and joint ventures (past 3 years)	
A list of members from the extended management team	
A list of members from the commercial teams	

Sampling Files

In phase 2 of the testing, the assessors request the following documents for a selected sample.

Sampling Baseline CMS Principles	Status
<i>For a sample of active sales and commercial intermediaries, provide:</i>	
- Formal commitment (e.g. contract, compliance declaration) to prevent any AB & AT risks	
<i>For a sample of high-risk function employees, provide:</i>	
- Due diligence records	
<i>For a sample of sales employees, provide:</i>	

- Annual performance evaluation	
- Remuneration records	
<i>For a sample of employees, provide:</i>	
- Attendance records for AB & AT training	

Sampling Risk Assessment for Banknote Specific Risks	Status
<i>For a sample of sales and commercial intermediaries depending on the risk scoring, provide:</i>	
- Evidence of adequate risk classification (in the risk assessment template)	
- Internal & external due diligence questionnaires	
- Due diligence screening	
- Contractual agreements stipulating certain contractual provisions	
- Approval of the contract by Senior Management or delegates	
- A selection of activity reports	
- Compliance confirmation	
- Evidence of training	
- Justification for special pricing (only applicable for distributors/resellers)	
- Special approval for remuneration over threshold	
- Approval of deviating payment	
- Risk assessment sign-off	
- External due diligence (only when applicable)	
- Contract sign-off	
- Evidence of additional mitigations	
<i>For a sample of hired former government officials or PEPs depending on the risk scoring, provide:</i>	
- Evidence of adequate risk classification and supporting documentation (in the risk assessment template)	
- Hiring report	
- Evidence of consultation with the compliance function	
- Meeting minutes of all interactions between the organization and the relevant former government official or PEP	
- Evidence that a second company representative who is not a former government official or PEP joined the conversation	
<i>For a sample of interactions/contracts with competitors depending on the risk scoring, provide:</i>	
- Evidence of adequate risk classification and supporting documentation (in the risk assessment template)	
- Attendance records or completion rate of AT specific trainings	
- Evidence of communication of checklists with do's and don'ts when interacting with government officials to all relevant people	
- Signed declaration between applicant/member and competitor before discussions	
- Evidence of the decision regarding the requirement of third-party presence	
- Due diligence process and due diligence clauses regarding AT risks in the contract	

Sampling Minimum Standards	Status
<i>For a sample of members of the extended management team and commercial teams, provide:</i>	
- Signed Annual Compliance Conformity Declaration	
<i>For a sample of employees, provide:</i>	
- Records and approvals of non-trivial gifts, hospitality and travel	
- Evidence of appropriate trainings followed	
- Last performance evaluation	
- Contractual clauses on AB & AT policies and disciplinary action, including termination rights	
<i>For a sample of past mergers, acquisitions and joint ventures, provide:</i>	
- Due diligence procedures	
<i>For a sample of sales and commercial intermediaries, provide:</i>	
- Approval by compliance before contract sign-off	

Overview of all sales intermediaries							
	Sales Intermediary	Country ²⁸	Remuneration Model	Commission %	Remuneration / Year and % of Contract Value		
					Year 1	Year 2	Year 3
1.	<i>Agent A</i>						
2.	<i>Agent B</i>						
3.	<i>Agent C</i>						
4.	...						
5.							
6.							
7.							
8.							
9.							
10.							
....							

Overview of all resellers/distributors						
	Sales Intermediary	Country ²⁹	Remuneration Model	Total Remuneration % for Product / Year		
				Year 1	Year 2	Year 3
1.	<i>Reseller/distributor A</i>					
2.	<i>Reseller/distributor B</i>					
3.	<i>Reseller/distributor C</i>					
4.	...					

²⁸ In which the intermediary operates to represent or support the member/applicant.

²⁹ In which the reseller/distributor operates to represent or support the member/applicant.

5.						
6.						
7.						
8.						
9.						
10.						
....						

5.4 INTERVIEW LIST

BnEI 2.0 | Interview List

Function-based interview list: The roles (or equivalent) included in this list must be interviewed by the assessors based on their function.

BnEI 2.0 <i>Function-based</i> Interview List	
Function	
	Compliance officer
	Risk manager
	Sales director
	Human resource manager
	Chief audit executive
	Finance & accounting manager (or e.g. treasury officer, controller)
	Procurement manager
	IT manager
	High risk sales and commercial intermediaries

*Please note that if the specific role does not exist in your organization, an equivalent role must be selected.

Population based interview list: The assessors will make a selection from the populations included in this list.

BnEI 2.0 <i>Population based</i> Interview List	
Function	
	Local compliance representatives
	Member(s) of senior management
	A selection of employees
	Member(s) of the governing committee
	Key managers in relevant functional areas ³⁰
	Member(s) of the extended management team and commercial team

*Please note that if the specific role does not exist in your organization, an equivalent role must be selected.

³⁰ Relevant functional areas of the business are including but not limited to: compliance, finance, sales, procurement and human resources.

5.5 SAMPLING GUIDE

BnEI 2.0 | Sampling Guide

This sampling guide provides general recommendations for determining sample sizes in the context of effectiveness testing of certain measures implemented by the applicant/member. The guidance considers both the size of the population and the assessed risk level (high, medium, or low) based on assessors judgement. The population size is determined over the entire audit scope period, which concerns three years (36 months) in case of a full audit and one year (12 months) in case of a partial re-audit, starting from the first month after the previous audit period.

Special provisions are made for very small populations. If the population size is 2 to 10 items, a minimum of 2 to 4 items is advised depending on the risk, with full population testing recommended if the number of required samples exceeds the available items. When the population consists of a single item, full population testing is automatically applied.

These sampling thresholds serve as a practical reference point and should be adapted when needed, based on professional judgment of the assessor, the nature of the control or transaction being tested, and the results of prior testing. Depending on the deviations or failures identified in the samples tested, the sample size may need to be extended to ensure sufficient coverage and reliability of the audit conclusions. Ultimately, the aim is to ensure a level of assurance that is both cost-effective and aligned with audit quality standards.

Population size	High risk	Medium risk	Low risk
> 500	40	30	25
100-500	25	20	15
10-100	15 *Full population if less than 15 samples	10 *Full population if less than 10 samples	5
2-10	4 *Full population if less than 4 samples	3 *Full population if less than 3 samples	2
= 1	1	1	1

This guide provides general recommendations and should be adapted based on the specific circumstances of the audit. Assessors should use their professional judgment to ensure the sampling approach is appropriate and aligned with audit objectives.

5.6 ANNUAL LETTER OF CONFIRMATION

BnEI 2.0 | Letter of Confirmation

“Pass” Accreditation

In case of a consistent “Pass” grading across all audit aspects, the audit will be performed every three years. A completed version of this template letter of confirmation must be provided to the assessors 12 and 24 months after accreditation. It must be signed by the CEO and General Counsel (or equivalent).

“Improvement Recommended” Accreditation

Members who were accredited with an “Improvement Recommended” grading in one or multiple aspects, must undergo a partial re-audit in the year N+1 to ensure the required mitigation measures were taken. If, following the re-audit, the member has moved to a “Pass” Accreditation, they will be required to complete a version of this template letter of confirmation 24 months after accreditation. It must be signed by the CEO and General Counsel (or equivalent).

FOR THOSE MEMBERS WITH AN “IMPROVEMENT RECOMMENDED” OUTCOME

Dear [],

We confirm that during the period from [DATE OF ACCREDITATION] to [CURRENT DATE] there have been no material changes to:

- The nature of the operations of the organizations which were included in the scope of the initial audit.
- The structure and the members of management team without suitable replacements having been recruited or being in the process of recruitment.
- The policies and procedures which were reviewed at the time of the accreditation audit, with the exception of those procedures modified as a result of an “improvement recommended” outcome in the final audit report.
- The ISO37001 accreditation status (if applicable).

[IF ANY OF THE ABOVE HAVE BEEN SUBJECT TO MATERIAL CHANGES PLEASE PROVIDE INFORMATION WHICH DESCRIBES THE CHANGE AND THE REASON FOR IT WITH RELEVANT DOCUMENTARY EVIDENCE]

We confirm the following steps have been/are being taken to mitigate any outstanding improvement points relating to the baseline CMS principles in the last 12 months.

[COMPANY TO DETAIL ACTIONS TAKEN TO MITIGATE ‘IMPROVEMENT POINTS’ REGARDING THE BASELINE CMS PRINCIPLES]

We confirm that there has been no acquisition, merger, or joint venture participation which has taken place during the same period which has had a significant impact on the application and functioning of the processes and procedures of the company.

[COMPANY TO DESCRIBE DETAILS OF SIGNIFICANT IMPACT AS NECESSARY]

[IF THE COMPANY HAS BEEN SUBJECT TO A MERGER, HAS FORMED A NEW JOINT VENTURE, HAS BEEN WHOLLY OR PARTIALLY ACQUIRED OR HAS ACQUIRED ANY OTHER COMPANY SINCE THE INITIAL AUDIT PLEASE PROVIDE DETAILS OF THIS, OF THE NEW OWNERS AND OF HOW THIS HAS AFFECTED OPERATIONS AND PROCESSES. EXAMPLES OF THIS INCLUDE IF THE COMPANY HAS BEEN REQUIRED TO ABIDE BY THE NEW OWNER’S POLICIES OR IF THE COMPANY HAS NOT FOR ANY REASON APPLIED ITS OWN/EQUIVALENT POLICIES TO THE NEW ACQUISITION OR JOINT VENTURE]

We confirm that during the same period, no action has been undertaken which may compromise the reputation or the credibility of the accreditation to the Banknote Ethics Initiative or the reputation or the credibility of the BnEI scheme itself, including dissemination of negative rumours about other members within the scheme.

Yours truly,

For and on behalf of: _____

Signature: _____

Printed name: _____

Position: _____

Date: _____

FOR THOSE MEMBERS WITH A “PASS” ACCREDITATION

Dear [],

We confirm that during the period from [DATE OF ACCREDITATION] to [CURRENT DATE] there have been no material changes to:

- The nature of the operations of the organizations which were included in the scope of the initial audit.
- The structure and the members of management team without suitable replacements having been recruited or being in the process of recruitment.
- The policies and procedures which were reviewed at the time of the accreditation audit.
- The ISO37001 accreditation status (if applicable).

[IF ANY OF THE ABOVE HAVE BEEN SUBJECT TO MATERIAL CHANGES PLEASE PROVIDE INFORMATION WHICH DESCRIBES THE CHANGE AND THE REASON FOR IT WITH RELEVANT DOCUMENTARY EVIDENCE]

We confirm that there has been no acquisition, merger, or joint venture participation which has taken place during the same period which has had a significant impact on the application and functioning of the processes and procedures of the company.

[COMPANY TO DESCRIBE DETAILS OF SIGNIFICANT IMPACT AS NECESSARY]

[IF THE COMPANY HAS BEEN SUBJECT TO A MERGER, HAS FORMED A NEW JOINT VENTURE, HAS BEEN WHOLLY OR PARTIALLY ACQUIRED OR HAS ACQUIRED ANY OTHER COMPANY SINCE THE INITIAL AUDIT PLEASE PROVIDE DETAILS OF THIS, OF THE NEW OWNERS AND OF HOW THIS HAS AFFECTED OPERATIONS AND PROCESSES. EXAMPLES OF THIS INCLUDE IF THE COMPANY HAS BEEN REQUIRED TO ABIDE BY THE NEW OWNER’S POLICIES OR IF THE COMPANY HAS NOT FOR ANY REASON APPLIED ITS OWN/EQUIVALENT POLICIES TO THE NEW ACQUISITION OR JOINT VENTURE]

We confirm that during the same period, no action has been undertaken which may compromise the reputation or the credibility of the accreditation to the Banknote Ethics Initiative or the reputation or the credibility of the BnEI scheme itself, including dissemination of negative rumours about other members within the scheme.

For and on behalf of: _____

Signature: _____

Printed name: _____

Position: _____

Date: _____