Part III

Policy papers

III.1 Corporate Governance practices for Insurance Companies

III.2 Outsourcing Arrangements

III.1 Corporate Governance practices for Insurance companies

This policy paper is applicable to all licensed insurance companies operating in or from Aruba and is issued pursuant to section 10 of the State Ordinance on the Supervision of the Insurance Business (AB 2000 no. 82) (SOSIB).

1. Introduction

Insurance companies face special challenges, since they differ from other companies in that most of the funds they put at risk belong to third parties. Using third-party funds to generate income for the benefit of shareholders of a supervised institution demands that some limitation be placed by the supervisory authority on how prudently these funds can be put at risk.

It is essential that the management of the insurance company and its board of supervisory directors fully understand the nature of the business being undertaken by the company and the related risks, and are suitably qualified and competent to perform the necessary functions and oversight of the operation. In order to meet this goal, insurance supervisory authorities have developed a keen interest in determining that these institutions adopt sound corporate governance practices. These practices are presented below and the Centrale Bank van Aruba (the Bank) aims at promoting the adoption of sound corporate governance practices by insurance companies subject to its supervision.

2. Basic elements of sound corporate governance practices

Basic elements of sound corporate governance practices are:

- Establish clear strategic objectives and corporate values that are communicated throughout the organization.
- Set and enforce clear lines of responsibility and accountability throughout the organization.
- Ensure that board members and senior-management are qualified for their positions.
- Install adequate risk management policies.
- Implement comprehensive internal controls.
- Provide for full, accurate and timely financial disclosure.

In the following paragraphs these elements will be discussed more in length, especially in relation to the responsibilities of the Board.

3. Responsibilities of the board and its members

The Board has dual responsibilities. The Board has its responsibilities as a whole, while each Supervisory Director has responsibilities as an individual member of the Board.
The responsibilities of the Board as a whole can be summarized as follows:

- Ensure competent management on an ongoing basis.
- Ensure appropriate plans and policies for the institution.
- Monitor operations to ensure compliance and adequate control.
- Oversee business performance.

3.1 Board responsibilities

A. To ensure competent management on an ongoing basis

Capable management is a critical element in the difference between success and failure of on institution. Integrity and suitability should be key considerations in the selection process of senior-management. Reference is made to paragraph 2 of the Directive on Sound Business Operations for further information on the integrity and suitability assessment conducted by the Bank. The appointment or dismissal of a member of senior-management should have the approval or at least the consent of the Board.

B. To ensure appropriate plans and policies for the institution

Planning

Rapid changes in the insurance industry call for clear strategies and business planning. Long-term strategic planning is done in strong cooperation with the Board and forms the broad policy framework, containing the institution's philosophy and vision to the future.

Policies

All major activities must be covered by adequate policies and no such activity should be initiated before appropriate written policies and procedures are in place. Furthermore, policies should be communicated clearly through all levels, in order to promote consistency of interpretation throughout the organization as a whole. Reference is also made to paragraph 3 of the Directive on Sound Business Operations.

C. To monitor operations to ensure compliance and adequate control

The Board needs to ensure that senior-management has put adequate internal controls in place to ensure that the institution's operations are properly controlled and that they comply with adopted policies, applicable laws and regulations.

D. To oversee business performance

The Board must receive timely all necessary information to evaluate management's performance (refer also to paragraph IV.3). The information provided should include at least:

- quarterly balance sheet and profit and loss account;
- analysis of actual versus budgeted income and costs (also per insurance branche);
- analysis of key ratio's and trends (including prudential ratio's);

- information on accounting, policy and compliance matters;
- information on important external developments;
- internal audit reports (including management's comments);
- reports from and correspondence with the external auditor (including the so-called management-letter);
- on-site examination letter and other relevant correspondence with the supervisor; and,
- changes in relevant laws and regulations;

3.2 Supervisory director's individual responsibilities

A Supervisory Director should:

A. be aware of the institution's operating environment

Each Supervisory Director should be generally informed of both the business environment and the legal and regulatory framework affecting the institution's activities.

B. be diligent in performing its duties

Supervisory Directors must devote adequate time and attention necessary to fulfill their duties in a proper manner and should be knowledgeable enough to contribute in a meaningful sense to the activities of the Board.

C. exercise independent judgment

If a Supervisory Director disagrees with a Board decision, he or she should say so and formally register and explain his or her disagreement. Objective judgment, with due observance of the articles 9 and 10 of the Directive on Sound Business Operations, is critical to the Board's effectiveness.

D. be loyal to the institution's interests

Supervisors Directors are responsible for protecting the institution's interests. They must also ensure that neither they nor others abuse their position to benefit personally from the institution and avoid even the appearance of a conflict of interest. Reference is also made to articles 9 and 10 of the Directive on Sound Business Operations.

3.3 Required qualifications

Candidates for board positions in supervised insurance companies need at least some basic knowledge of either insurance or financial accounting. However, the Board as a whole must possess sufficient knowledge and experience in the insurance field.

3.4 Separate Board Committees

The Board can form, for example, the following separate committees, in order to perform certain tasks that require detailed review or in-depth consideration.

Audit Committee:	This committee serves to monitor for compliance with Board's policies, applicable laws and regulations, and to review financial and auditing matters.
Risk Management Committee:	This committee ensures that acceptable risk limits and that appropriate risk-control techniques are in place to monitor and minimize losses to the institution.
Investment Committee:	This committee ensures that the institution's investment policies and assets/liabilities mix are adequate and that the institution's investments comply with Board policies, general principles of asset and liability management, principles of risk management, and applicable laws and regulations.
Personnel development Committee:	Matters usually dealt with by this committee include CEO compensation arrangements, remuneration, recruitment and termination policies, incentive schemes, and remuneration arrangements for Board members.

It should be stressed, however, that the Board as a whole remains fully responsible for a proper supervision of the institution. Therefore, these committees should report to the complete Board on all major issues discussed.

4. Risk Management

When evaluating the quality of risk management at insurance companies, the Bank considers primarily if the following conditions are met:

- active Board and senior-management oversight;
- adequate policies, procedures, and limits;
- adequate risk measurement, monitoring, and management information systems; and
- adequate and comprehensive internal controls.

4.1 Active Board and senior-management oversight

The Board should be consulted on the overall business strategy and on significant policy matters, including those related to the managing and taking of risks.

Senior-management is, however, primarily responsible for implementing strategies in a manner that limits risks associated with each strategy and that ensures compliance with laws and regulations on both a long-term and a day-to-day basis.

4.2 Adequate policies, procedures, and limits

The following guidelines are considered by the Bank in evaluating the adequacy of a supervised institution's policies, procedures, and limits:

- The institution's policies, procedures, and limits provide for adequate identification, measurement, monitoring, and control of the risks posed by its activities.
- The policies, procedures, and limits are consistent with the institution's stated goals and objectives and the overall financial strength of the institution.
- Policies clearly delineate accountability and lines of authority across the institution's activities.
- Policies provide for the review of new activities of the financial institution to ensure that the infrastructure necessary to identify, monitor, and control risks associated with an activity is in place before the activity is initiated.

4.3 Adequate risk measurement, monitoring, and management information systems

Effective risk monitoring requires institutions to identify and measure all material risk exposures. Consequently, risk monitoring activities must be supported by information-systems that provide senior-managers and Board with timely reports on the financial condition, operating performance, and risk exposure of the financial institution, as well as with regular and sufficiently detailed reports for line managers in the day-to-day management of the institution's activities.

In assessing the adequacy of a supervised institution's measurement and monitoring of risk and its management reports and information systems, the Bank will consider whether the following conditions exist:

- The institution's risk monitoring practices and reports address all of its material risks.
- Key assumptions, data sources, and procedures used in measuring and monitoring risk are appropriate and adequately documented and tested for reliability on an ongoing basis.
- Reports and other forms of communication are consistent with the institution's activities, structured to monitor exposures and compliance with established limits, goals, or objectives, and as appropriate, compare actual versus expected performance.
- Reports to the Board and management are accurate and timely and contain sufficient information to identify any adverse trend and to evaluate adequately the level of risk faced by the institution.

4.4 Comprehensive internal controls

An institution's internal control environment is critical to the safe and sound functioning of the institution and, in particular, to its risk management system. Establishing and maintaining an effective system of controls, including appropriate segregation of duties, is one of senior-management's primary responsibilities.

When properly structured, a system of internal controls promotes effective operations and reliable financial and regulatory reporting. Moreover, the system safeguards assets and helps to ensure compliance with relevant laws, regulations, and institutional policies.

An internal auditor should test internal controls regularly. The results of audits or reviews should be adequately documented, as should management's responses to them. In addition, communication channels should exist that allow negative or sensitive findings to be reported directly to the Board or to the relevant Committee of the Board.

III.2 Outsourcing Arrangements

Policy Paper issued on the basis of sections 15 and 15a of the State Ordinance on the Supervision of the Credit System (SOSCS), sections 10 and 10a of the State Ordinance on the Supervision of the Insurance Business (SOSIB), section 11a of the State Ordinance on Company Pension Funds (SOCPF), and section 21 of the State Ordinance on the Supervision of the Securities Business (SOSSB).[1]

1. Introduction

Outsourcing arrangements may increase the risk profile of an institution due to, for example, reputation, compliance and operational risks arising from failure of a service provider in providing the service, breaches in security, or the institution's inability to comply with legal and regulatory requirements. An institution can also be exposed to country risk, when a service provider is located overseas, and concentration risk, when more than one service is outsourced to the same service provider. Outsourcing does not diminish the obligations of an institution, and those of its Supervisory Board and Managing Board, to comply with the relevant laws and regulations in Aruba. In this regard, it is important that an institution adopts a sound and responsive risk management framework for all of its material outsourcing arrangements.

2. Scope and applicability of the Policy Paper

2.1 This Policy Paper is applicable to all companies and institutions that fall under the scope of the SOSCS, SOSIB, SOCPF and SOSSB. Any deviation from this Policy Paper must be explained in a separate document, to be made directly available to the Centrale Bank van Aruba (CBA) upon request. In case parts of this Policy Paper are not applicable, this must also be recorded in the aforementioned document. Institutions with a limited size (e.g. credit unions) or activities may request for a dispensation of the requirements set out in this Policy Paper, provided that these institutions have policies and procedures in place with regard to outsourced services insofar material that are considered sufficiently effective by the CBA.

2.2 This Policy Paper provides a set of standards on sound practices on risk management of outsourcing arrangements that institutions must follow. The extent and degree to which an institution implements these standards should be commensurate with the nature of risks in, and materiality of, the outsourcing arrangement. An institution must ensure that outsourced services continue to be managed as if the services were still managed by the institution.

2.3 Annex 1 provides a non-exhaustive list of examples of outsourcing arrangements to which this Policy Paper is applicable, and arrangements that are not intended to be

[1] This Policy Paper is largely based on a policy paper on outsourcing issued by the Monetary Authority of Singapore.

subject to this Policy Paper. It should also not be misconstrued that arrangements not defined as outsourcing need not be subject to adequate risk management and sound internal controls. Annex 2 provides guidance to an institution in assessing whether an outsourcing arrangement would be considered a material outsourcing arrangement. Annex 3 provides a template for an institution to maintain a register of its material outsourcing arrangements. This register must be made directly available to the CBA upon request.

3. Definitions

3.1 In this Policy Paper, unless the context otherwise requires:

3.1.1 Institution means:
Credit institutions, insurance companies, pension funds, securities brokers, asset managers, investment institutions, custodians and stock exchanges, supervised by virtue of the SOSCS, SOSIB, SOCPF and SOSSB;

3.1.2 Material outsourcing arrangement means an outsourcing arrangement:
(a) Which, in the event of a service failure or security breach, has the potential to either significantly impact an institution's:
(i) business operations, reputation or profitability, or
(ii) ability to manage risk and comply with applicable laws and regulations, or
(b) Which involves customer information and, in the event of any unauthorized access or disclosure, loss or theft of customer information, may have a significant impact on an institution's customers;

3.1.3 Outsourcing agreement means:
A written agreement setting out the contractual terms and conditions governing relation-ships, obligations, responsibilities, rights and expectations of the contracting parties in an outsourcing arrangement;

3.1.4 Outsourcing arrangement means:
An arrangement in which a service provider provides the institution with a service that may currently or potentially be performed by the institution itself and which includes the following characteristics:
(a) The institution is dependent on the service on an ongoing basis; and
(b) The service is integral to the provision of a financial service by the institution or the service is provided to the market by the service provider in the name of the institution;

3.1.5 Service provider means:
Any party which provides a service to the institution, including any entity within the institution's group [2], whether it is located in Aruba or elsewhere;

[2] This refers to the institution's Head Office or parent institution, subsidiaries, affiliates, and any entity (including their subsidiaries, affiliates and special purpose entities) that the institution exerts control over or that exerts control over the institution.

3.1.6 Sub-contracting means:
An arrangement where a service provider which has an outsourcing agreement with an institution, further outsources the services or a material part of the services covered under the outsourcing arrangement to another service provider.

4. Risk management practices

4.1 Responsibility of the Supervisory Board and Managing Board

4.1.1 The Supervisory Board and Managing Board of an institution play pivotal roles in ensuring a sound risk management culture and environment. While an institution may delegate day-to-day operational duties to the service provider, the responsibilities for maintaining effective oversight and governance of outsourcing arrangements, managing outsourcing risks, and implementing an adequate outsourcing risk management framework, in accordance with this Policy Paper, continue to rest with the institution, its Supervisory Board and Managing Board. The Supervisory Board and Managing Board of an institution must ensure that there are adequate processes to provide a comprehensive institution-wide view of the institution's risk exposures from outsourcing, and incorporate the assessment and mitigation of such risks into the institution's outsourcing risk management framework.

4.1.2 The Managing Board is responsible for:

(a) Establishing a framework to evaluate the risks and materiality of all existing and prospective outsourcing arrangements and the policies that apply to such arrangements;
(b) Developing sound and prudent outsourcing policies and procedures that are commensurate with the nature, scope and complexity of the outsourcing arrangements as well as ensuring that these policies and procedures are implemented effectively
(c) Setting a suitable risk appetite to define the nature and extent of risks that the institution is willing and able to assume from its outsourcing arrangements;
(d) Laying down appropriate approval authorities for outsourcing arrangements consistent with its established strategy and risk appetite;
(e) Assessing management competencies for developing sound and responsive outsourcing risk management policies and procedures that are commensurate with the nature, scope, and complexity of the outsourcing arrangements;
(f) Undertaking regular reviews of outsourcing strategies and arrangements for their continued relevance, safety and soundness; and
(g) Communicating information pertaining to risks arising from its material outsourcing arrangements to the Supervisory Board in a timely manner.

4.1.3 The Supervisory Board is responsible for:

(a) Evaluating the materiality and risks from all existing and prospective outsourcing arrangements, based on the framework established by the Managing Board;

(b) Reviewing regularly the effectiveness of, and appropriately adjusting of, policies, standards, and procedures to reflect changes in the institution's overall risk profile and risk environment;
(c) Monitoring and maintaining effective control of all risks from its material outsourcing arrangements on an institution-wide basis;
(d) Ensuring that contingency plans, based on realistic and probable disruptive scenarios, are in place and regularly tested;
(e) Ensuring that there is independent review and audit for compliance with outsourcing policies and procedures; and
(f) Ensuring that appropriate and timely remedial actions are taken to address audit findings.

4.2 Evaluation of risks

4.2.1 In order to be satisfied that an outsourcing arrangement does not result in the risk management, internal control, business conduct or reputation of an institution being compromised or weakened, the Supervisory board and Managing Board need to be fully aware of and understand the risks arising from outsourcing. The institution must establish a framework for risk evaluation which should include the following steps:
(a) Identifying the role of outsourcing in the overall business strategy and objectives of the institution;
(b) Performing comprehensive due diligence on the nature, scope, and complexity of the outsourcing arrangements to identify and mitigate key risks;
(c) Assessing the service provider's ability to employ a high standard of care in performing the outsourced service and meet regulatory standards as if the outsourcing arrangement is performed by the institution;
(d) Analyzing the impact of the outsourcing arrangement on the overall risk profile of the institution, and whether adequate internal expertise and resources are available to mitigate the risks identified;
(e) Analyzing the institution's as well as the institution's group aggregate exposure to the outsourcing arrangement, to manage concentration risk; and
(f) Analyzing the benefits of outsourcing against the risks that may arise, ranging from the impact of temporary disruption to service, to that of a material breach in security and confidentiality, and unexpected termination of the outsourcing arrangement, and whether for strategic and internal control reasons, the institution should not enter into the outsourcing arrangement.

4.2.2 Such risk evaluations should be performed when an institution is planning to enter into a material outsourcing arrangement with an existing or a new service provider, and also re-performed periodically on existing material outsourcing arrangements, as part of the approval, strategic planning, risk management or internal control reviews of the outsourcing arrangements of the institution.

4.3 Assessment of Service Providers

4.3.1 In considering renegotiating or renewing an outsourcing arrangement, an institution should subject the service provider to appropriate due diligence processes to assess the risks associated with the outsourcing arrangement.

4.3.2 An institution must assess all relevant aspects of the service provider, including its capability to employ a high standard of care in the performance of the outsourcing arrangement as if the service is performed by the institution to meet its obligations as a regulated entity.

The due diligence must also take into account the physical and IT security controls the service provider has in place, the business reputation and financial strength of the service provider, including the ethical and professional standards held by the service provider, and its ability to meet obligations under the outsourcing arrangement. On-site visits at the service provider, and where possible, independent reviews and market feedback on the service provider, must also be obtained to supplement the institution's assessment. On-site visits must be conducted by persons who possess the requisite knowledge and skills to conduct the assessment.

4.3.3 The due diligence must involve an evaluation of all relevant information about the service provider. Information to be evaluated includes the service provider's:

(a) Experience and capability to implement and support the outsourcing arrangement over the contracted period;
(b) Financial strength and resources (the due diligence should be similar to a credit assessment of the viability of the service provider based on reviews of business strategy and goals, audited financial statements, the strength of commitments of major equity sponsors and the ability to service commitments even under adverse conditions);
(c) Corporate governance, business reputation and culture, compliance, and pending or potential litigation;
(d) Security and internal controls, audit coverage, reporting and monitoring environment;
(e) Risk management framework and capabilities in respect of the outsourcing arrangement;
(f) Disaster recovery arrangements and disaster recovery track record;
(g) Reliance on sub-contractors;
(h) Insurance coverage;
(i) External environment (such as the political, economic, social and legal environment of the jurisdiction in which the service provider operates); and
(j) Ability to comply with applicable laws and regulations, and track record in relation to its compliance with applicable laws and regulations.

4.3.4 The service provider must ensure that the employees of the service provider undertaking any part of the outsourcing agreement have been assessed to meet the institution's hiring policies for the role they are performing, consistent with the criteria that are applicable to the institution's own hiring criteria. Any adverse

findings from this assessment should be considered in light of their relevance and impact to the outsourcing arrangement.

4.3.5 Due diligence undertaken during the assessment process should be documented and re-performed periodically as part of the monitoring and control processes of material outsourcing arrangements. The due diligence process may vary depending on the nature, extent of risks of the arrangement, and impact on the institution in the event of a disruption to service or breach of security and confidentiality (e.g., reduced due diligence may be sufficient where the outsourcing arrangements are made within the institution's group) [3]. An institution must ensure that the information used for due diligence evaluation is sufficiently current. An institution must also consider the findings from the due diligence evaluation to determine the frequency and scope of audit on the service provider.

4.4 Outsourcing Agreement

4.4.1 Contractual terms and conditions governing relationships, obligations, responsibilities, rights, and expectations of the contracting parties in the outsourcing arrangement must be carefully and properly defined in written agreements.

4.4.2 An institution must ensure that every outsourcing agreement addresses the risks identified during the risk evaluation and due diligence stages. Each outsourcing agreement should allow for timely renegotiation and renewal to enable the institution to retain an appropriate level of control over the outsourcing arrangement and the right to intervene with appropriate measures to meet its legal and regulatory obligations. It should, at the very least, have provisions to address the following aspects of outsourcing:

(a) Scope of the outsourcing arrangement;
(b) Performance, operational, internal control and risk management standards;
(c) Confidentiality and security [4];
(d) Business continuity management [5];
(e) Monitoring and control [6];
(f) Audit and inspection [7];
(g) Notification of adverse developments: an institution must specify in its outsourcing agreement the type of events and the circumstances under which the service provider should report to the institution;
(h) Dispute resolution: an institution must specify in its outsourcing agreement the resolution process, events of default, the indemnities, remedies and recourse of the respective parties in the agreement. The institution should ensure that its contractual rights can be exercised in the event of a breach of the outsourcing agreement by the service provider;

---

3 In case of outsourcing within the same group, the institution must have a Service Level Agreement in place for the outsourced services. Refer to paragraph 4.10.
4 Refer to paragraph 4.5.
5 Refer to paragraph 4.6.
6 Refer to paragraph 4.7.
7 Refer to paragraph 4.8.

(i) Default termination and early exit: an institution must have the right to terminate the outsourcing agreement in the event of default, or under circumstances where:
   (i) the service provider undergoes a change in ownership;
   (ii) the service provider becomes insolvent or goes into liquidation;
   (iii) the service provider goes into receivership or judicial management;
   (iv) there has been a breach of security or confidentiality; or
   (v) there is a demonstrable deterioration in the ability of the service provider to perform the contracted service.

The minimum period to execute a termination provision must be specified in the outsourcing agreement. Other provisions must also be put in place to ensure a smooth transition when the agreement is terminated or being amended. Such provisions may facilitate transferability of the outsourced services to a third party. Where the outsourcing agreement involves an intra-group entity, the agreement should be legally enforceable against the intra-group entity providing the outsourced service;

(j) Sub-contracting: an institution must retain the ability to monitor and control its outsourcing arrangements when a service provider uses a sub-contractor. An outsourcing agreement must contain clauses setting out the rules and limitations on sub-contracting. An institution must include clauses making the service provider contractually liable for the performance and risk management practices of its sub-contractor and for the sub-contractor's compliance with the provisions in its agreement with the service provider. The institution must ensure that the sub-contracting of any part of material outsourcing arrangements is subject to the institution's prior approval;

(k) Applicable laws: agreements must include choice-of-law provisions, agreement covenants and jurisdictional covenants that provide for adjudication of disputes between the parties under the laws of a specific jurisdiction.

4.4.3 Each outsourcing agreement must be tailored to address issues arising from country risks and potential obstacles in exercising oversight and management of the outsourcing arrangements made with a service provider outside of Aruba.

4.5 Confidentiality and Security

4.5.1 As public confidence in institutions is a cornerstone in the stability and reputation of the financial industry, it is vital that an institution satisfies itself that the service provider's security policies, procedures, and controls will enable the institution to protect the confidentiality and security of customer information.

4.5.2 An institution must be proactive in identifying and specifying requirements for confidentiality and security in the outsourcing arrangement. An institution must take the following steps to protect the confidentiality and security of customer information:

(a) State the responsibilities of contracting parties in the outsourcing agreement to ensure the adequacy and effectiveness of security policies and practices, including the circumstances under which each party has the right to change security requirements. The outsourcing agreement should also address:

(i) the issue of the party liable for losses in the event of a material breach of security or confidentiality and the service provider's obligation to inform the institution; and

(ii) the issue of access to and disclosure of customer information by the service provider. Customer information should be used by the service provider and its staff strictly for the purpose of the contracted service;

(b) Disclose customer information to the service provider only on a need-to-know basis;

(c) Ensure the service provider is able to protect the confidentiality of customer information, documents, records, and assets, particularly where multi-tenancy[8] arrangements are present at the service provider; and

(d) Review and monitor the security practices and control processes of the service provider on a regular basis, including commissioning audits or obtaining periodic expert reports on confidentiality, security adequacy and compliance in respect of the operations of the service provider, and requiring the service provider to disclose to the institution breaches of confidentiality in relation to customer information.

4.6 Business Continuity Management

4.6.1 An institution must ensure that its business continuity is not compromised by outsourcing arrangements, in particular, of the operation of its critical systems.

4.6.2 An institution must take steps to evaluate and satisfy itself that the interdependency risk arising from the outsourcing arrangement can be adequately mitigated in such a way that the institution remains able to conduct its business with integrity and competence in the event of a service disruption or failure, or unexpected termination of the outsourcing arrangement or liquidation of the service provider. These should include taking the following steps:

(a) Determine that the service provider has in place satisfactory business continuity plans (BCP) that are commensurate with the nature, scope, and complexity of the outsourcing arrangement. Outsourcing agreements should contain requirements on the service provider in the area of business continuity, in particular, recovery time objectives (RTO), recovery point objectives (RPO), and resumption operating capacities;

(b) Proactively seek assurance on the state of business continuity preparedness of the service provider. It should ensure that the service provider regularly tests its BCP and that the tests validate the feasibility of the RTO, RPO, and resumption of the operating capacities. The institution should require the service provider to notify it of any test findings that may affect the service provider's performance. The institution should also require the service provider to notify it of any substantial changes in the service provider's BCP and of any adverse development that could substantially impact the service provided to the institution; and

[8] Multi-tenancy generally refers to a mode of operation adopted by service providers where a single computing infrastructure (e.g., servers, databases etc.) is used to serve multiple customers (tenants).

(c) Ensure that there are plans and procedures in place to address adverse conditions or termination of the outsourcing arrangement such that the institution will be able to continue business operations and that all documents, records of transactions and information previously given to the service provider are promptly removed from the possession of the service provider or deleted, destroyed or rendered unusable, with due regard to the applicable legislation in the country where the service provider is located.

4.6.3 For assurance on the functionality and effectiveness of its BCP, an institution should design and carry out regular, complete and meaningful BCP testing that is commensurate with the nature, scope and complexity of the outsourcing arrangement.

4.6.4 The institution must consider worst case scenarios in its BCP. Some examples of these scenarios are unavailability of the service provider due to unexpected termination of the outsourcing agreement, liquidation of the service provider and wide-area disruptions that result in collateral impact on both the institution and the service provider.

4.7 Monitoring and Control

4.7.1 An institution must establish a structure for the management and control of its outsourcing arrangements. Such a structure will vary depending on the nature and extent of risks in the outsourcing arrangements. As relationships and interdependencies in respect of outsourcing arrangements increase in materiality and complexity, a more rigorous risk management approach should be adopted. An institution also has to be more proactive in its relationship with the service provider (e.g., having frequent meetings) to ensure that performance, operational, internal control, and risk management standards are upheld.

4.7.2 An institution must put in place all of the following measures for effective monitoring and control of any material outsourcing arrangement:

(a) Maintain a register of all material outsourcing arrangements and ensure that the register is readily accessible for review by the Supervisory Board and Managing Board of the institution and the CBA. The information maintained in the register must at a minimum consist of the information set out in Annex 3.

(b) Assign clear responsibilities within the institution for the monitoring and controlling of the outsourcing agreement;

(c) Periodic reviews on all material outsourcing arrangements. This is to ensure that the institution's outsourcing risk management policies and procedures, and the requirements in this Policy Paper, are effectively implemented. Such reviews must ascertain the adequacy of internal risk management and management information systems established by the institution (e.g., assessing the effectiveness of processes and metrics used to evaluate the performance and security of the service provider) and highlight any deficiency in the institution's systems of control;

(d) Reporting policies and procedures: reports on the monitoring and control activities of the institution must be reviewed by its Managing Board, while the outcome must be shared with the Supervisory Board. The institution must also ensure that any adverse development arising in any outsourcing arrangement is brought to the immediate attention of the Managing Board of the institution and service provider, and where warranted, to the institution's Supervisory Board. When adverse development occurs, prompt actions should be taken by an institution to review the outsourcing relationship for modification or termination of the agreement.

4.8 Audit and Inspection

4.8.1 An institution's outsourcing arrangements must not interfere with the ability of the institution to effectively manage its business activities or impede the CBA in carrying out its supervisory functions and meeting its objectives.

4.8.2 An institution must include, in all of its outsourcing agreements for material outsourcing arrangements, clauses that:

(a) Allow the institution to conduct audits on the service provider, whether by its internal or external auditors, or by agents appointed by the institution; and to obtain copies of any report and finding made on the service provider, whether produced by the service provider's internal or external auditors, or by agents appointed by the service provider, in relation to the outsourcing arrangement;

(b) Allow the CBA, where necessary or expedient, to exercise the contractual rights of the institution to:

(i) access and inspect the service provider, and obtain records and documents, of transactions, and information of the institution given to, stored at or processed by the service provider; and

(ii) access any report and finding made on the service provider, whether produced by the service provider's internal or external auditors, or by agents appointed by the service provider, in relation to the outsourcing arrangement.

4.8.3 Outsourcing agreements for material outsourcing arrangements must also include clauses that require the service provider to comply, as soon as possible, with any request from the CBA or the institution, to the service provider or its sub-contractors, to submit to the CBA any report on the security and control environment of the service provider and its sub-contractors, in relation to the outsourcing arrangement.

4.8.4 An institution must ensure that independent audits and/or expert assessments of all its material outsourcing arrangements are conducted. In determining the frequency of audit and expert assessments, the institution should consider the nature and extent of the involved risks, and the impact on the institution from the outsourcing arrangements. The scope of the audit and expert assessments should include an assessment of the service provider's security [9] and control environment, incident

[9] The security environment refers to both the physical and IT security environments.

management process (for material breaches, service disruptions or other material issues) and the institution's observance of this Policy Paper in relation to the outsourcing arrangement.

4.8.5 The independent audit and/or expert assessment on the service provider may be performed by the institution's internal or external auditors, the service provider's external auditors [10] or by agents appointed by the institution. The appointed persons should possess the requisite knowledge and skills to perform the engagement, and be independent of the unit or function performing the outsourcing arrangement.
The Supervisory Board must ensure that appropriate and timely remedial actions are taken to address the audit findings [11]. Institutions must have adequate processes in place to ensure that remedial actions are satisfactorily completed.

4.8.6 Significant issues and concerns must be brought to the attention of the Managing Board of the institution and service provider, and where warranted, to the Supervisory Board. Actions must be taken by the institution to review the outsourcing arrangement if the risk posed is no longer within the institution's risk tolerance.

4.8.7 Copies of audit reports must be directly submitted by the institution to the CBA upon request. An institution must also, upon request, provide the CBA with other reports or information on the institution and service provider that is related to the outsourcing arrangement.

4.9 Outsourcing outside Aruba

4.9.1 The engagement of a service provider in a foreign country, or an outsourcing arrangement whereby the outsourced function is performed in a foreign country, may expose an institution to country risk (economic, social and political conditions and events in a foreign country) that may adversely affect the institution. Such conditions and events could prevent the service provider from carrying out the terms of its agreement with the institution. In its risk management of such outsourcing arrangements, an institution must take into account, as part of its due diligence:

(a) Government policies;
(b) Political, social, and economic conditions;
(c) Legal and regulatory developments in the foreign country; and
(d) The institution's ability to effectively monitor the service provider, and execute its business continuity plans and exit strategy.

The institution must also be aware of the disaster recovery arrangements and locations established by the service provider in relation to the outsourcing arrangement. As information and data could be moved to primary or backup sites located in foreign countries, the risks associated with the medium of transport, be it physical or electronic, should also be considered.

[10] An institution should conduct its own audits to supplement the audits performed by the service provider's auditors, where necessary.
[11] Refer to paragraph 4.1.

4.9.2 Material outsourcing arrangements with service providers located outside of Aruba must be conducted in a manner so as not to hinder the CBA's efforts to supervise the Aruban business activities of the institution (i.e., from its books, accounts and documents) in a timely manner, in particular:

(a) An institution may not enter into outsourcing arrangements with service providers operating in jurisdictions that do not uphold confidentiality clauses and agreements; and

(b) An institution may not enter into outsourcing arrangements with service providers in jurisdictions where prompt access to information by the CBA at the service provider may be impeded by legal or administrative restrictions.

4.10 Outsourcing within a group

4.10.1 This Policy Paper is also applicable to outsourcing arrangements with parties within an institution's group. The expectations may be addressed within group-wide risk management policies and procedures. The institution would be expected to provide, when requested, information demonstrating the structure and processes by which its Supervisory Board and Managing Board discharge their role in the oversight and management of outsourcing risks on a group-wide basis.

4.10.2 Due diligence on an intra-group service provider may take the form of evaluating qualitative aspects of the service provider's ability to address risks specific to the institution, particularly those relating to business continuity management, monitoring and control, audit and inspection, including confirmation on the right of access to be provided to the CBA, to retain effective supervision over the institution, and compliance with local regulatory standards. The respective roles and responsibilities of each office in the outsourcing arrangement should be documented in writing in a Service Level Agreement.

4.11 Outsourcing of Internal Audit to External Auditors

4.11.1 Where the outsourced service is the internal audit function of an institution, there are additional factors that an institution should take into account. One of these is the lack of independence, or the appearance of impaired independence, when a service provider is handling multiple engagements for an institution, such as internal and external audits, and consultancy services. There is doubt that the service provider, in its internal audit role, would criticize itself for the quality of the external audit or consultancy services provided to the institution. In addition, as operations of an institution could be complex and involve large transaction volumes and amounts, it should ensure service providers have the expertise to adequately complete the engagement. An institution should address these and other relevant issues before outsourcing the internal audit function. In addition, as a sound practice, institutions shall not outsource their internal audit function to the institution's external audit firm.

4.11.2 Before outsourcing the internal audit function to external auditors, an institution must satisfy itself that the external auditor is in compliance with the relevant standards, including the independency standards, regulating the accounting profession.

This Policy Paper enters into force on **July 1, 2018**.

Annex 1

EXAMPLES OF OUTSOURCING ARRANGEMENTS

1 The following are examples of some services that, when performed by a third party, would be regarded as outsourcing arrangements for the purposes of this Policy Paper although they are not exhaustive:

(a) Application processing (e.g., loan origination, insurance underwriting, credit cards);

(b) Middle and back office operations (e.g., electronic funds transfer, payroll processing, custody operations, quality control, purchasing, maintaining the register of participants of a collective investment scheme (CIS) and sending of accounts and reports to CIS participants, order processing, trade settlement and risk management);

(c) Business continuity and disaster recovery functions and activities;

(d) Claims administration (e.g., loan negotiations, loan processing, insurance claim processing, collateral management, collection of bad loans);

(e) Document processing (e.g., cheques, credit card and bill payments, bank statements, other corporate payments, customer statement printing);

(f) Information systems hosting (e.g., software-as-a-service, platform-as-a-service, infrastructure-as-a-service);

(g) Information systems management and maintenance (e.g., data entry and processing, data centers, data center facilities management, end-user support, local area networks management, help desks, information technology security operations);

(h) Investment management (e.g., discretionary portfolio management, cash management);

(i) Management of policy issuance and claims operations (by managing agents);

(j) Manpower management (e.g., benefits and compensation administration, staff appointment, training and development);

(k) Marketing and research (e.g., product development, data warehousing and mining, media relations, call centers, telemarketing);

(l) Professional services related to the business activities of the institution (e.g., accounting, internal audit, actuarial, compliance);

(m) Support services related to archival, storage and destruction of data and records; and

(n) Cloud computing.

2 The following arrangements would generally **not** be considered outsourcing arrangements, falling under the scope of this Policy Paper:

(a) Arrangements in which certain industry characteristics require the use of third party providers;
  (i) maintenance of custody accounts;
  (ii) telecommunication services and public utilities (e.g., electricity, SMS gateway services);
  (iii) postal services;
  (iv) market information services (e.g., Bloomberg, Moody's, Standard & Poor's);
  (v) common network infrastructure (e.g., Visa, MasterCard);
  (vi) clearing and settlement arrangements between clearing houses and settlement institutions and their members, and similar arrangements between members and non-members;
  (vii) global financial messaging infrastructure which are subject to oversight by relevant regulators (e.g., SWIFT); and
  (viii) correspondent banking services.

(b) Introducer arrangements and arrangements that pertain to principal-agent relationships:
  (i) sale of insurance policies by agents, and ancillary services relating to those sales;
  (ii) acceptance of business by underwriting agents; and
  (iii) introducer arrangements (where the institution does not have any contractual relationship with customers).

(c) Arrangements that the institution is not legally or administratively able to provide:
  (i) statutory audit and independent audit assessments;
  (ii) discreet advisory services (e.g., legal opinions, independent appraisals, trustees in bankruptcy, loss adjuster); and
  (iii) Independent consulting (e.g., consultancy services for areas which the institution does not have the internal expertise to conduct).

Annex 2

MATERIAL OUTSOURCING ARRANGEMENTS

1 An institution should assess the materiality in an outsourcing arrangement. In assessing materiality, the CBA recognizes that qualitative judgment is involved and the circumstances faced by individual institutions may vary. Factors that an institution should consider include:

(a) Importance of the business activity to be outsourced (e.g., in terms of contribution to income and profit);
(b) Potential impact of the outsourcing on earnings, solvency, liquidity, funding, capital, and risk profile;
(c) Impact on the institution's reputation and brand value, and ability to achieve its business objectives, strategy, and plans, should the service provider fail to perform the service or encounter a breach of confidentiality or security (e.g., compromise of customer information);
(d) Impact on the institution's customers, should the service provider fail to perform the service or encounter a breach of confidentiality or security;
(e) Impact on the institution's counterparties and the Aruban financial market, should the service provider fail to perform the service;
(f) Cost of the outsourcing as a proportion of total operating costs of the institution;
(g) Cost of outsourcing failure, which will require the institution to bring the outsourced activity in-house or seek similar service from another service provider, as a proportion of total operating costs of the institution;
(h) Aggregate exposure to a particular service provider in cases where the institution outsources various functions to the same service provider; and
(i) Ability to maintain appropriate internal controls and meet regulatory requirements, if the service provider faces operational problems.

2 Outsourcing of all or substantially all of its risk management or internal control functions, including compliance, internal audit, financial accounting and actuarial (other than performing certification activities) is to be considered a material outsourcing arrangement.

3 An institution should undertake periodic reviews of its outsourcing arrangements to identify new outsourcing risks as they arise. An outsourcing arrangement that was previously not material may subsequently become material from incremental services outsourced to the same service provider or an increase in volume or change in nature of the service outsourced to the service provider. Outsourcing risks may also increase when the service provider subcontracts the service or makes significant changes to its sub-contracting arrangements.

4 An institution should consider materiality at both the institution's level and as a group, i.e. together with the institution's branches and corporations under its control.

Annex 3

REGISTER OF MATERIAL OUTSOURCING ARRANGEMENTS [12]

An institution should maintain an updated register of all existing material outsourcing arrangements. The register must - at a minimum - contain the following information:

(a) Name of service provider / sub-contractor as set out in the outsourcing agreement;
(b) Description of outsourced service(s);
(c) Contract renewal date (where applicable);
(d) Service expiry (date);
(e) Date that the institution undertook due diligence on the outsourcing / sub-contracting arrangement; and
(f) Date that an independent audit was last conducted on the service provider / sub-contractor.

[12] Refer to paragraph 4.7.