Guidance to implement the requirements of the International Financial reporting Standard (17)

Subject Contents Page

Introduction

In May 2017, the International Accounting Standards Board (IASB) issued a new standard on insurance contracts, which was to be introduced as of 1/1/2021 and which would replace the currently applied International Financial Reporting Standard (4). The application of the standard requirements was subsequently postponed until 1/1/2023 in June 2020.

The International Financial Reporting Standard (IFRS 17) represents a comprehensive change in accounting for insurance contracts, which will enhance the transparency of the actual financial performance of insurance companies, and aims to make corporate financial statements more realistic in measuring results and recognizing revenues and liabilities and be more comparable across insurance companies.

The standard covers accounting aspects of a wide range of contracts issued by insurance companies, and the effect of this standard varies depending on the type of contracts held by each company. The greatest impact will be on long-term insurance contracts. However, the change will be fundamental to all insurance companies.

Implementing the requirements contained in the new standard will result in changes in the operations of insurance companies, which will require insurance companies to change the accounting processing methods they use, their financial reporting mechanism and the need for them to modify and develop systems and restructure their operations. New principles apply to accounting for insurance contracts (including recognizing expected losses), which requires insurance companies to prepare policies, procedures and decisions that ensure that the company can best apply the standard's requirements.

IFRS 17 relies on taking into account the time value of money when measuring liabilities to reflect the current value of future cash flows, using a discount rate that reflects the risks to the company, and is reviewed and updated frequently.

This guide has been prepared to assist insurance companies in implementing the requirements of IFRS 17, taking into account the complexity and proprietary nature of the operations of insurance companies, as well as increasing transparency and ensuring that appropriate and objective financial data is displayed. This guide describes the requirements for the general implementation of IFRS 17, the requirements of information security systems, details of the accounting policy which will describe the application of IFRS 17 by the company, and requirements for

central bank approval. This reflects the interest of the central bank to ensure that insurance companies observe the minimum requirements stated in the standard and appropriate information is provided to the central bank.

Chapter I
Implementation of IFRS 17

First: Definition of contract

- In order for a company to meet the requirements of the standard, a company must prepare a board-approved policy that enables it to determine whether or not the contract complies with the definition of an insurance contract contained in the standard.
- The policy referred to above shall include the minimum:
  - Definition of insurance contract
  - Identify contracts issued by a company that are consistent with the definition of an insurance contract.
  - Identify contracts issued by a company that do not conform to the definition of an insurance contract
  - Definition of fundamental insurance risks.
  - Mechanism for determining the relative importance of insurance contract risks.

Second: Separating the components of the insurance contract

- In order for the company to meet the standard requirements, the company must study the contracts it has written and ensure that there are no components in those contracts that do not comply with the standard and which can be separated. Where applicable, the Company must ensure that components can be separated and processed to the most relevant standard according to a policy to separate the components of the Insurance Contract approved by the Board of Directors.
- The policy referred to above shall include the minimum:
  - Mechanism for separating non-insurance components from insurance contract.
  - The most appropriate standard to be applied to the treatment of non-insurance components.
  - Mechanism for determining the relative importance of the components of an insurance contract.

Third: The level of aggregation

- In order to meet the requirements of the standard, the company must prepare a board-approved policy to collect insurance contracts in separate portfolios that are separately written and processed, divided into three levels, respectively:

  1) Similar risks.
  2) Year of underwriting.
  3) Profitability.

- Level 1 (similar risk)

  General Insurance companies must collect portfolios of insurance contracts according to the same risk as those contracts and to the minimum as follows:
  - Compulsory Motor Insurance portfolio.
  - Comprehensive Motor insurance portfolio.
  - Bus pool insurance portfolio.
  - Engineering Insurance portfolio.
  - Tender portfolios that extend for more than a year.
  - The rest of other insurance portfolios according the standard requirement.

- Level 2 (year of underwriting)

  The company should classify the portfolios of insurance contracts into groups by year of underwriting example (all contracts issued during Financial Year 2020 are treated separately from those issued in Financial Year 2021 and so on).

- Level 3 (profitability)

  The company shall classify the portfolios of insurance contracts into groups based on the net cash flows expected from the contract and apply the accounting approach followed in the handling of the contract sets as hereinafter referred to in this manual:
  - Contracts that have no possibility of becoming onerous upon initial recognition.
  - Onerous contracts.
  - Other contracts, if any.

Fourth: Recognition of the insurance contract

- In order for the company to meet the requirements of the standard, the company must recognize a group of insurance contracts as at the following dates, whichever is earlier:
  1) The beginning of the coverage period.
  2) The date at which the first payment is due.
  3) When the contract becomes Onerous.

Fifth: future cash flows

- Future cash flows are defined as all amounts expected to be collected and expected to be paid resulting from insurance contracts, and they must be estimated upon recognition of the insurance contract based on a policy approved by the Board of Directors that includes actuarial assumptions and the company's experience in managing a group of insurance contracts, where future cash flows include at least the following :
  1) Expected future cash flows (Cash Inflow)
     - Written premiums, taking into account the mechanism of payment of those premiums specified in the insurance contract.
     - Revenues related to the insurance contract, such as fees for issuing insurance contracts.
     - Revenue from expected recoveries and debris.
  2) Expected future cash flows (Cash Outflow)
     - Best estimate of the cost of claims incurred, and claims that have occurred but not reported.
     - Claims expected to be incurred, including payments arising from non-insurance components that cannot be separated from the contract.
     - Administrative and personnel expenses associated with insurance contracts.
     - Allocation of cash flows for acquisition costs.
     - Costs incurred in providing non-financial services (Motor maintenance, home rebuilding).
     - Claims handling costs (inspector of losses, judicial expenses).
  3) Future cash flows that must be excluded from any estimation:
     - Cash flows arising under retained reinsurance contracts such as commissions received and interest paid on retained balances.
     - Investment revenues.
     - The cash flows that may arise from future insurance contracts.
     - The cash flows arising from the separate components of the insurance contract.

- Cash flows that are not related to the insurance contract portfolio.

- The company should consider the aspects set out below when making assumptions related to the process of estimating the future cash flows of groups of insurance contracts:
  - Inherent risk.
  - Level of aggregation.
  - The possibility of natural disasters.
  - The possibility of liquidating the contract before the date of expiry of the insurance coverage, and other practices expected of the insurance contract holder.
  - The factors that will affect the estimates, and the sources of information for these factors.

Sixth: Acquisition costs

- In order for the company to meet the requirements of the standard, the company must prepare a policy approved by the board of directors and evaluated by the actuary appointed by the company, enabling it to allocate acquisition costs according to the group of insurance contracts, and the way they are handled, to include at least the following:
  - Mechanism for estimating acquisition costs when preparing estimated budgets.
  - The mechanism of amortizing acquisition costs.
- The insurance company is obligated to defer the recognition of acquisition costs, to be recorded in the statement of financial position, and extinguished according to the mechanism adopted in the policy referred to above.

Seventh: The discount rate

- In order for the company to meet the requirements of the standard, the company must prepare a policy approved by the board of directors to determine the discount rate and be evaluated by the actuary appointed by the company, provided that it includes, at a minimum, the following:
  - Determine the mechanism used in calculating the discount rate.
  - The mechanism for reviewing the hypotheses used in calculating the discount rate.
  - That the discount rate be consistent with market prices, and reflect the time value of money and the characteristics of cash flows and liquidity characteristics in insurance contracts.

- The discount rate must be compatible with the currency in which the contract liabilities recorded.
- Determine the yield curve used to discount cash flows.

- The discount rate is applied to the cash flows when calculating the following items:
  - Liabilities for incurred claims (claims expected to be paid within more than 12 months).
  - Liabilities for remaining coverage (general approach / variable fee).

Eighth: Adjustments for non-financial risks

- In order for the company to meet the requirements of the standard, the company must prepare a policy approved by the board of directors for calculating non-financial risk adjustments for each group of insurance contracts. It is to be determined as part of the risk management policy to be evaluated by the actuarial expert appointed by the company. The policy includes, at a minimum, the following :
  - Defining non-financial risks.
  - Determining the method to be followed in monitoring the value of adjustments for non-financial risks.
  - The level of confidence used to calculate the value of adjustments for non-financial risks.
- Also, when calculating the value of adjustments for non-financial risks, the following must be excluded:
  - Operational risks.
  - The risks of matching assets and liabilities.
  - Pricing risk.
  - Credit risk related to assets corresponding to insurance contract liabilities.
- In order for the company to meet the requirements of the standard, the company must explicitly include the value of adjustments for non-financial risks when calculating the following items:
  - Liabilities for incurred claims.
  - Liabilities for remaining coverage (general approach / variable fee).

Ninth: Contract Measurement Approaches

- The standard provides insurance companies with three approaches to measuring and treating insurance contracts and reinsurance contracts that are held for accounting, which are as follows:

1) General Approach
   Applied to all insurance contracts, as it requires measuring the liabilities of groups of insurance contracts by discounting the future cash flows "incoming and outgoing" and then subtracting from them the non-financial risk adjustments to arrive at the contractual service margin, which represents the unearned profit from the group of insurance contracts.
2) Premium allocation method
   Applies to the groups of insurance contracts shown below:
   - The term of insurance coverage does not exceed one year.
   - In which the value of the "Liabilities for remaining coverage" does not materially differ from its value when applying the requirements of the general approach.

   Taking into account that a discount rate should be used to calculate the present value of the cash flows if the method is applied to a group of contracts with a coverage period of more than one year, according to the aforementioned exception.
3) Variable fee approach
   It is the approach by which some of the requirements of the general approach are modified for the treatment of investment contracts, including those with the benefit of participation.

- In order for the company to meet the requirements of the standard, the company must prepare a policy for measuring and treating insurance contracts and reinsurance contracts held, approved by the Board of Directors, and evaluated by the actuary appointed by the company, including at least the following:
  - Insurance contracts that will be processed according to the requirements of the premium allocation approach, the general approach and/or the variable fee approach.
  - The mechanism for testing the applicability of the premium allocation approach according to the level of materiality in cases where the coverage period is more than one year.
  - The mechanism for determining the level of relative importance used in testing the application of the premium allocation method.

Tenth: Disclosures

The company shall disclose in its financial statements, in addition to what is stated in paragraphs (93) to (132) of the standard, at a minimum, the following aspects:

1) Adjustments between the opening balance and the closing balance of the liabilities item against the remaining coverage, in a way that shows the present value of future cash flows, risk adjustments, contractual service margin, financing expense/revenue for each portfolio separately. In addition, the loss component should be clarified in the event of onerous contracts within the insurance contract groups.
2) Adjustments between the opening balance and the closing balance of the liabilities item against the claims incurred in a way that shows the present value of future cash flows, risk adjustments, financing expense, for each portfolio separately.
3) The discount rates used in calculating the present value of future cash flows, the method used and the factors that were relied upon in calculating those rates. In addition to the justifications for adopting the method used in calculating discount rates.
4) With regard to the impact of the transition to the standard, for contracts measured under the modified retrospective approach or the fair value approach upon transition to IFRS 17, the contractual service margin adjustment and insurance revenue amounts must be separately disclosed for contracts under each approach, in addition to reasons for using these approaches.
5) Management's estimates regarding the assumptions used in the following aspects:
   - Estimate the cash flow.
   - Level of aggregation.
   - Testing the application of the premium allocation approach to contracts whose coverage period exceeds one year.
   - Non-financial risk adjustments.
   - Mechanism for handling acquisition costs.
   - Separation of insurance contracts.
   - The method of processing the expenses/financing income.
   - The accounting methods used for each portfolio separately.
   - Any changes in the assumptions used for the items above.
6) Contracts issued by the company that do not meet the requirements of the standard.

Chapter II.
Manage IT system operations

First, manage the IT systems project for implementing IFRS 17

- In order for the company to manage the project more efficiently and effectively, the company must develop a board-approved business plan that is tailored to the nature of the company's business and the complexity of the requirements of IFRS 17, including the distribution of supervision and control functions and responsibilities over the stages of project implementation, the necessary reporting process, and risk assessment throughout the project period.
- In preparing the above-mentioned business plan, the company should consider the following aspects:
  1) The adequacy and efficiency of available resources (expertise, liquidity, human resources, etc.), including IT provider resources, to effectively implement the project.
  2) Coordination of the different departments of the company associated with the application of the requirements of IFRS 17.
  3) Examination of the aspects of the prospective IT system that are relevant to the requirements of IFRS 17 in the context of the nature of the business of the company
  4) The adequacy of the security and controls used in the prospective IT system to mitigate cyber security risks or data breaches.
  5) The management reports that the company needs to evaluate its performance and that the prospective IT system will need to produce, as well as determine the periodicity of the extraction of those reports.
  6) Timely recovery of existing data from IT system providers.
  7) The location of backups (which need to be safe and accessible when needed), and the mechanism for checking them.
  8) Appropriate procedures for disaster recovery and periodic testing.

Second: Details of the prospective IT system

- When the IT provider is approved by the board of directors, the company must ensure, as a minimum, that the system is able to handle the aspects below:
  - Data storage and archiving at the level necessary to meet IFRS 17 calcuation, reporting and disclosure requirements.
  - Applying the methods specified by IFRS 17 that are appropriate for the nature of a company's business.
  - Estimation of all future cash flows relevant to the company’s business, consistent with the assumptions relevant to them and inputed to the system.

- Calculating the current value of these cash flows according to the inputed discount rate policy.
- Separately calculating, reporting and disclosing the components of the insurance contract liabilities relating to (where relevant) the present value of future cash flows, the risk adjustment for non-financial risk, contractual service margin, and any loss component..
- Separately calculating, reporting and disclosing reinsurance contracts held.
- All administrative reports required by the board, management, or central bank.

- The following aspects of IT system audits should be extended to prospective IT systems for IFRS 17, subject to the relevant legislation in force. :
  - Ensure that internal audit personnel are adequately aware of the best practices for auditing IT systems generally, and the requirements for implementing IFRS 17 specifically.
  - The Internal Audit Service to prepare an IT audit report. The summary of the findings and corrective actions should be provided to the central bank on an annual basis. The report should contain all relevant documentation and verification of the adequacy of the approved internal control and control systems, and indicate the scope and methodology of the audit. and

Chapter III.
Rules for sharing and storing information with a third party

The following aspects of sharing and storing information with a third party should be extended to prospective IT systems for IFRS 17.

First: The minimum rules to be observed when sharing and storing information with a third party:

Contractual and legal aspects	
A company should use a risk based assessment methodology to determine which data is permitted to be stored or processed outside the company according to the nature, classification, and degree of data risk, subject to compliance with the relevant legislation in force.	1
The IT systems service provider must be known and reputable, and have no improper practices with those who work with or have worked with them.	2
A Service Level Agreement and Non-Disclosure Agreement with the IT service provider should be made, with agreements to define the standards by which operations are carried out by the IT service provider. The agreements should include penal and criminal provisions for any action or conduct that violates the privacy and security of information.	3
Information should be kept confidential so that it complies with the provisions of confidentiality of information under the Insurance Organization Act No. 12 of 2021 and the relevant legislation.	4
The company should ensure that its IT service provider has adequate controls to enable the company to meet its contractual and legal obligations, such as maintaining data privacy and reporting compliance with security and control controls.	5
Incident response procedures must be established to ensure that all incidents to which data may be exposed are dealt with effectively in a timely manner.	6
The company must assess the efficiency and effectiveness of the cloud computing service and its compatibility with information security requirements.	7

The company can either use the cloud computing service directly from the IT service provider or through an intermediary that the IT service provider uses. In the case of an intermediary, the company must consider the application of all applicable security and regulatory requirements as if the service was provided directly by the IT service provider.	8
The company should confirm the information privacy requirements when the contract with the IT service provider or intermediary ends, whether it is terminated or transferred to another service provider. All data, including backups, must be deleted by the IT service provider or intermediary after delivery to the company.	9
Manage data access	
Logical access and identity verification mechanisms must be used to access data stored by the IT service provider, which prohibits the granting of broad access permissions that result in unauthorized device/user access to data.	1
The company must create a secure and encrypted trunk to the IT service provider through a Virtual Private Network (VPN), especially when the connection is Site-to-Site.	2
Some sensitive protocols, such as SSH and RDP, should not be used over the internet without adequate and appropriate controls to prevent unauthorized use of data access methods.	3
Data protection	
The company should make sure that the data stored by the IT service provider is kept separate from data of other clients of the IT service provider through necessary isolation mechanisms, such as Multi-Tenant Environment.	1
The company must encrypt data during network traffic and when it is stored on servers, storage, and backups, taking into account the use of secure and acceptable encryption algorithms and protocols.	2
The company must set appropriate controls on encryption keys, and if its IT service provider is granted access to encryption keys, the responsibility for the data remains with the company.	3

The company must ensure that system/service assurance at the IT service provider is not exposed to any of the ten OWASP-related threats.	4
The company must ensure that all systems are protected through Anti-Virus/Anti-Malware Software, and that an Intrusion Prevention System is installed to prevent any interference or activity that damages data.	5
The company must ensure that a Web Application Firewall is used to minimize vulnerabilities or stop attacks on web applications.	6
The company must ensure that all applications, systems and devices are enhanced by System Harding controls in accordance with best practices.	7
Physical protection	
The company or IT service providermust keep the servers and IT systems infrastructure equipment in a safe place.	1
The company must ensure physical protection against external threats.	2
The company must ensure backup and business continuity plan are provided to sustain the business.	3
The company must ensure that a disaster recovery plan includes all possible disaster scenarios and is periodically tested.	4
Identity and Authentication Element Protection (Credentials)	
The company should ensure that the two-factor authentication method is used for all accounts to enhance protection when using username and password.	1
The company should never use accounts with absolute authority (built-in Administrator) as such authorities should only be used for certain actions that require them and only and in an emergency. Where absolute authorities are more generally used they should be replaced with accounts dedicated to work-needed powers (Least Privileges)	2
Shared accounts are prohibited. User names and private passwords must be created according to the Least Privilege principle, and tasks and powers must be separate.	3
The company should ensure that best practices in password policy and standards and session management are applied.	4
The company should ensure that application programming interface passwords and security keys are protected and changed periodically.	5

Security and audit records	
The company should ensure that security event logs and alerts are enabled to include for generated accounts (at least) event description, date and time, and that records are reviewed to monitor and detect suspicious movements and identify abnormal activities.	1
The company must ensure that the IT service provider alerts and notifies the company if any third parties request access to the data.	2
The company must ensure timely access to the necessary records for criminal investigation and investigation, and reporting of information relevant to the specific data or applications of the company.	3

Second: The minimum guiding rules to be adopted:

Contractual and legal aspects	
The company or IT service provider should periodically perform a Penetration Testing and Vulnerability Assessment, and the results should be reported to the company.	1
The company should ensure that a scenario-based risk assessment and planning activity is periodically performed to: - Identify ways that unauthorized access to data might be allowed. - Analyze the effectiveness of existing blocking and detection controls to reduce the likelihood of unauthorized access to data. - Analyze the probability and impact of Significant and Plausible Attack Vectors being employed in light of the controls used. - Analyze the effectiveness of the response controls used to reduce the impact of the Significant and Plausible Attack Vectors. - Identify the need for additional safeguards or disclosure.	2
The company should ensure that employees of the IT Service Provider and the Company Data Management team are appropriately qualified and experienced, and that their tasks are performed efficiently and effectively.	3
Manage data access	
Appropriate controls must be established and restricted to manage the internet access process (i.e. Restricted Public IP). The public access authorities (global access) should not be activated.	1

The company should ensure that mutual authentication or binary authentication is used to allow access to stored data.	2
Data protection	
The company should be aware that encryption is a fail-safe process so that a cryptographic mechanism/tool failure or security control failure does not affect encrypted data, and that unauthorized third parties have access to data that is unreadable and unusable.	1
The company should assess the information security requirements applied to the IT service provider, ensuring that data security standards are complied with, performing the Penetration Testing and Vulnerability Scanning, and continually assessing risk.	2
Identity and Authentication element Protection (Credentials)	
The company should ensure that a mechanism to continuously audit users' accounts and authority and cancel or disable unused accounts is adopted.	1
The company must ensure that the name of the account is considered for all accounts and assets, and that the name of the account does not indicate the powers granted.	2
Security and audit records	
The company should ensure that technologies that constantly monitor and check applicable security settings are used periodically.	1
The company should ensure that best practices for Application Programming Interface are used for testing, auditing, and protection of abnormal activities.	2

Third: The most important criteria to be used in the field of cloud

The company must ensure that the following standards are applied

Standards	Subject
• Cobit • ISO/IEC 20000 • SAE 16 or ITIL Dependding on type of workload • ISO/IEC 27001 and ISO/IEC 27002 • ISO/IEC 27017 & ISO/IEC 27018 • ISO/IEC 38500 - it Governance • Cloud Security Alliance (CSA) Cloud Controls Matrix • National Institute of Standards and Technology (NIST) • Cybersecurity Framework (CSF)	Governance, risk management and compliance
• SSAE 16 • ISO/IEC 27000	Operational and commercial operations
• LDAP, SAML 2.0, OAuth 2.0, WS-Federation, OpenID Connect, SCIM • XACML • PKCS, X.9, OpenPG	Manage roles
• HTTPS, SFTP, VPN using IPsec or SSL • Oasis KMIP • US FIPS 140-2	Data and information protection
• ISO/IEC 27018	Privacy policies
• ISO/IEC 27033 or FIPS199/200 Standards	Network security and protection
• ISO/IEC 27002 • ISO/IEC 27017 & ISO/IEC 27018	Infrastructure security controls
• ISO/IEC 19086 • ISO/IEC 27004:2009, TM Forum TR 178, NIST Special Publication 800-55, CIS Consenssus Security Metrics V1.1.0, and Enisa Procure secure	Service level Agreement Security conditions

• CWE List • CSA Star Registry • PCI DSS • FedraMP Program	

Chapter IV
Administrative processes

First: Planning and Estimated Budgets

- The company should define the bases and assumptions for preparing the estimated budgets in proportion to the requirements of the standard to ensure that the administrative reports are compatible with the financial reports.

Second: Actuarial Operations

- The actuarial operations related to the requirements of the standard consist of the following:
  - Pricing of insurance contracts.
  - Determining the adequacy of the value of the insurance contract Liabilities.
  - Develop assumptions for the process of estimating future cash flows.
  - Evaluation of the profitability of the contract
  - Determine discount rates.
  - Determining the contractual service margin upon initial recognition and subsequent measurement.
  - Determining adjustments for non-financial risks at initial recognition and subsequent measurement, and the appropriate estimation method.
  - Level of aggregation.
  - Participate in the identification of key performance indicators.
  - Sensitivity analysis.

Third: risk management processes

- The company must have at least the following:
  1) Risk Management Committee.
  2) The risk management charter.
  3) Risk management policy.
  4) The acceptable level of risk.
  5) Risk control framework and risk self-assessment.
  6) Asset and liability interview management policy.
- The company must identify and measure the risks resulting from the change in the accounting and actuarial policies and other aspects related to the requirements of the standard, so that the risks are identified for each of the company's relevant departments.