PremiumTrust Bank

ISMS Legal and Regulatory Requirements Procedure

Classification: Internal
April 2023
Document Number: PTB/ISMS/ILRRP/A5-31

Status: Approved

Document Control Sheet

Version and Update History

Date	Document Version	Document Revision History	Document Author/Reviser
April 3, 2023	1.0	Document creation	Information & Cyber Security

Change Control

Change Clause/Frequency
The contents of this document are subject to change control on a twelve (12) months review cycle.

Contents

1 Introduction

PremiumTrust Bank has implemented an Information Security Management System (ISMS) in line with the ISO/IEC 27001 international standard for information security management.

In creating and maintaining an ISMS it is vital that a full understanding is gained of the various legal and regulatory requirements that apply to PremiumTrust Bank and its business. This will ensure that the organization continues to meet its obligations and its board of directors and other stakeholders are not exposed to the risk of criminal prosecution or corporate liability.

The purpose of this procedure is to document how such requirements are identified and incorporated into the ISMS and how updates to the requirements are handled.

2 Procedure

The procedure for identifying and managing legal and regulatory requirements is summarised in the diagram below. Each step is expanded upon in the following sections.
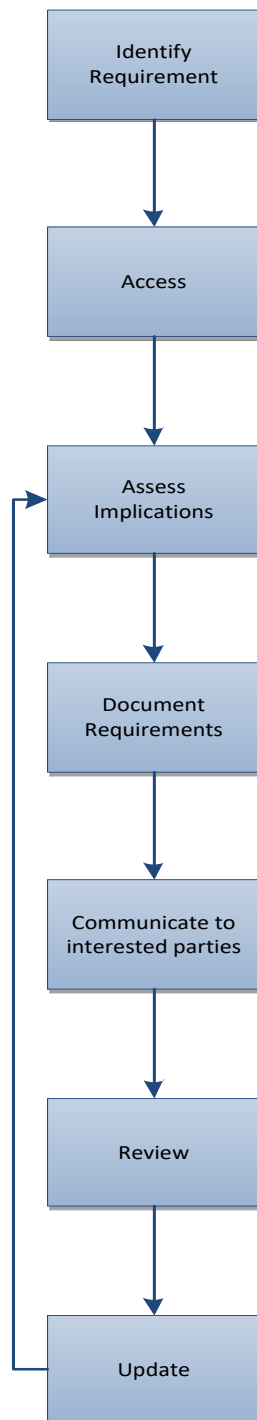
```
┌──────────────────┐
│    Identify      │
│   Requirement    │
└──────────────────┘
         │
         ▼
┌──────────────────┐
│     Access       │
└──────────────────┘
         │
         ▼
┌──────────────────┐
│     Assess       │ ◄──┐
│  Implications    │    │
└──────────────────┘    │
         │              │
         ▼              │
┌──────────────────┐    │
│    Document      │    │
│  Requirements    │    │
└──────────────────┘    │
         │              │
         ▼              │
┌──────────────────┐    │
│  Communicate to  │    │
│ interested parties│   │
└──────────────────┘    │
         │              │
         ▼              │
┌──────────────────┐    │
│     Review       │    │
└──────────────────┘    │
         │              │
         ▼              │
┌──────────────────┐    │
│     Update       │ ───┘
└──────────────────┘
```

Figure 1 – Legal and regulatory requirements procedure

2.1 Identify Requirement

PremiumTrust Bank relies upon the following internal teams and external bodies to identify legal and regulatory requirements that are relevant to its business operations:

Team	Areas Covered	Method of Communication
Operations Department	Compliance with Laws and Regulations	Email alerts Annual meetings
Infrastructure and Security	Data Protection	Email alerts Annual monthly meetings
Infrastructure and Security	Cybersecurity	Email alerts Annual meetings

Include all real or potential sources of advice in the above table.

2.2 Access

In general, PremiumTrust Bank will rely upon the appropriate team or external body to provide an interpretation of the relevant parts of the item under consideration. This may be in the form of briefing papers or presentation materials.

Where necessary, the Head of Operations shall obtain full copies of the relevant source material (such as Acts of Law or Regulatory announcements) for reference purposes. These may be in hardcopy or electronic form.

2.3 Assess Implications

The Head of Operations and the ISMS Manager is responsible for ensuring that a full assessment of the implications of the relevant items is carried out. This will be based upon qualified advice from the relevant source above. The assessment will include the following aspects:

- Degree of change to the ISMS and its associated policies. strategies and plans needed to meet the requirement.
- Urgency of meeting the requirement
- Consequences of not meeting the requirement
- Options for meeting the requirement.

2.4 Document Requirement

Once assessed, the relevant requirements will be documented as part of the ISMS within the document Information Security Context, Requirements and Scope. All changes to this document will be recorded in accordance with the ISMS documentation procedures.

Where possible, confirmation of the interpretation of the requirement will be obtained from a relevant source e.g. the organization Operations department.

2.5 Communicate to Interested Parties

Where immediate changes are needed to the ISMS as a result of a new or changed requirement these will be incorporated as soon as possible, and revisions issued to all recipients of the relevant policies and procedures. Otherwise, the change will be considered at the next annual review of the ISMS.

2.6 Review

All relevant requirements will be re-assessed on at least an annual basis as part of the ISMS annual review. Appropriate advice will be obtained at this point to ensure that all changes have been captured.

2.7 Update

Any new or changed requirements identified as part of the review will be handled in accordance with this procedure and appropriate updates made.