PremiumTrust Bank

Vendor Information Security Evaluation Procedure

Classification: Internal
April 2023
Document Number: PTB/ISMS/VISEP/A5.19

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.

1 Table of Contents

1.0 Introduction

The Vendor Information Security Evaluation Procedure sets out a process for the evaluation of the Information Security arrangements of our vendors so that a degree of confidence may be gained that they possess sufficient security to support PremiumTrust Bank's requirements.

It should be noted that this process is not intended to carry out a full risk assessment of vendors, rather to assess whether they have taken such action themselves and put in place adequate precautions to ensure continued security assurance.

Vendor Information Security Evaluation is applied to the Information Security Management System (ISMS) scope as defined in the Information Security Policy. Users of Vendor Information Security Evaluation are members of senior management and staff implementing the Information Security management system.

2 Vendor Information Security Evaluation Procedure

2.1 Process Diagram

The process of supplier Information Security evaluation is shown in the diagram below.

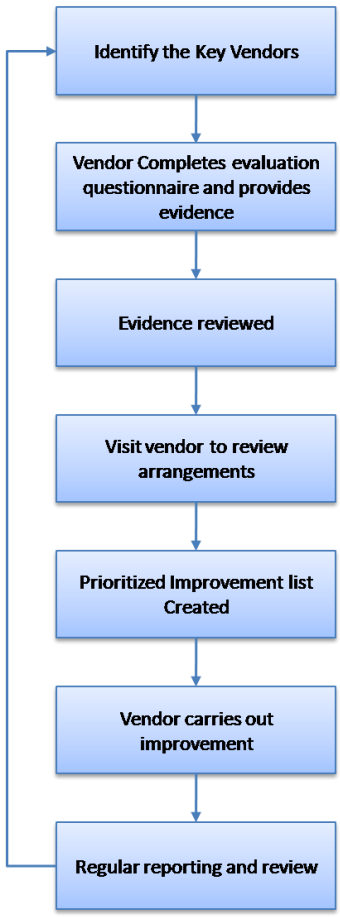

Fig 1 – Vendor Information Security Evaluation Process

Each step in this process is described in more detail in the rest of this document.

2.2 Process Inputs

The process of evaluating a vendor's Information Security arrangements starts with a number of inputs which are needed to ensure that all the steps can be completed successfully.
These inputs should include where available:

- Information Security Context, Requirements and Scope
- Information Security Policy
- Risk Assessment Report
- Service Level Agreement (SLA)
- Contract Agreements
- Legal and regulatory requirements

The availability of this information will ensure that the conclusions reached are based on factual data rather than mere approximations.

2.3 "Right-to-audit" Clauses in Contract Agreements13

As the outsourcing of business functions has become more popular, PremiumTrust Bank inevitably shares increasing amounts of data, which is often highly confidential, with external service providers.

Often, these service providers must use personal information supplied to them by their customers to provide the relevant services. This personal information may pertain to the customer's employees and contractors, its own customers, business partners or other third parties.

Therefore, PremiumTrust Bank must put in place appropriate contractual protections with each of its service providers having access to the customer's personal information to:

- Specify the service provider's standard of care and its obligations with respect to the treatment of personal information.
- Minimize the risks and liabilities associated with a service provider's security breach or the unauthorized use of personal information.

This provision grants PremiumTrust Bank the right to conduct or oversee an audit of the service provider's facilities and practices, more especially, if the service provider will have access to highly sensitive personal information.

Appendices 2 and 3 respectively provide a customizable sample of the "right-to-audit", and "Information Security and Continuity Requirements" clauses that must be included in all applicable contract agreements.

2.4 Identification of Key Vendors

The starting point for the process is to identify which vendors are critical to the delivery of the identified critical business activities for PremiumTrust Bank. and the processes that support them. This information is captured during the risk assessment and business impact assessment processes that are performed as part of the ISMS.

For more detail on these processes please see the following documents:

- PremiumTrust Bank Business Impact Analysis and Risk Treatment Process
- PremiumTrust Bank ISMS Risk Assessment and Risk Treatment Process
- PremiumTrust Bank Supplier Management Policy

For each critical business activity, the dependencies that support it are identified, including the specific products and services provided by each vendor.

This provides a list of vendors that will need to be assessed in the context of the products and services they offer (as not all aspects of the vendor's business operations will necessarily be relevant to the critical business activities of PremiumTrust Bank.

The evaluation of the list of vendors should be completed in priority order i.e., in the order of greatest risk to PremiumTrust Bank. This is designed to ensure that risk is minimized as quickly as possible.

A schedule of vendor evaluations should be created which considers available resources (of both PremiumTrust Bank and the vendors) and any seasonal considerations e.g., period of peak business.

2.5 Vendors Complete Evaluation Questionnaires and Provide Evidence

A main contact should be established with the vendor. This contact should be of sufficient authority within the vendor organization to ensure that the evaluation is given adequate priority and that all the required information can be provided.

The Information Security Evaluation questionnaire will be sent to the vendor contact requesting certain information.

A target date for the completed questionnaire and supporting information/evidence should be agreed with the vendor contact and reminders issued where needed.

2.6 Evidence Reviewed

Once received, the evidence provided by the vendor should be reviewed by the Business Continuity Coordinator or the designated evaluation officer in consultation with the relevant business line managers.

This review will aim to assess the residual level of risk to PremiumTrust Bank critical business activities, considering the adequacy of the vendor's business continuity arrangements.

2.7 Visit Supplier/Vendor to Review Arrangements

Where possible, a visit should be undertaken to the vendor site(s) most relevant to the supply of goods and services to PremiumTrust Bank. This visit is to:

- Verify the completeness and accuracy of the evidence provided.
- Discuss the improvements that may be required.
- Build a relationship with the vendor.
- Better understand the business environment

Several visits may be required depending on the geographical spread of locations, scope of product or service supply and availability of key vendor staff.

2.8 Prioritized Improvement List Created

A list of proposed improvements to the vendor's business continuity arrangements is then created. This list should be prioritized according to the level of risk and agreed upon with the main vendor contract. Commitment to target dates for completion should also be obtained and documented.

2.9 Vendor Carries out Improvements

The vendor is then given an opportunity to address the improvements on the agreed list to the target timescales. The frequency of regular progress updates should be agreed, and progress tracked against the plan. Failure to achieve the identified improvements within the target timescales should be discussed both with the vendor contact and senior management within PremiumTrust Bank and the level of risk assessed.

2.10 Regular Reporting and Review

In addition to a full annual review, vendor Information Security assessments will be evaluated regularly to ensure they remain current. The relevant assessments will also be reviewed regarding major changes to the business such as mergers and acquisitions or the introduction of new products and services.

2.11 Process Outputs

The process of vendor Information Security evaluation results in several outputs which show that all the steps have been completed successfully.

3 Roles and Responsibilities

Within the process of vendor Information Security evaluation there are several key roles that play a part in ensuring that all impacts are identified, addressed and managed. These roles are shown in the RACI chart below, together with their relative responsibilities at each stage of the process.

RACI Chart

The table below clarifies the responsibilities at each step using the RACI model, i.e.:

R= Responsible A= Accountable C= Consulted I= Informed

Role: **Step**	**Information Security Manager or Designated Evaluation officer**	**Business Line Manager**	**Vendor Contact**
Identification of Key Vendors	A	R	C
Vendor completes evaluation questionnaire and provides evidence	A	I	R
Evidence reviewed	A	R	I
Visit vendor to review arrangements	A	R	C
Prioritized improvement list created	A	R	C
Vendor carries out improvements	A	C	R
Regular Reporting and Review	A	R	C

Further roles and responsibilities may be added to the above table as the process matures within PremiumTrust Bank

Appendix 1: Sample "Right-to-audit" Clause

[PremiumTrust Bank Limited, hereafter referred to as Customer's [written] request, to confirm Service Provider's compliance with Agreement, as well as any applicable laws, regulations and industry standards, Service Provider grants Customer or, upon Customer's election, a third party on Customer's behalf, permission to perform an assessment, audit, examination or review of all controls in Service Provider's physical and/or technical environment in relation to all Personal Information being handled and/or services being provided to Customer pursuant to this Agreement. Service Provider shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports Personal Information for Customer pursuant to this Agreement. In addition, upon Customer's [written] request, Service Provider shall provide Customer with the results of any audit by or on behalf of Service Provider performed that assesses the effectiveness of Service Provider's information security program as relevant to the security and confidentiality of Personal Information shared during the course of this Agreement.]

Appendix 2: Sample-A "Information Security" Clause

The Receiving Party of any Customer Data of the Disclosing Party shall be responsible for establishing, implementing, maintaining and performing a reasonable information security program (including physical security of physical items) that is reasonably designed to (i) ensure the security and confidentiality of such Customer Data, (ii) protect against any anticipated threats or hazards to the security or integrity of such Customer Data, (iii) protect against unauthorized access to or use of such Customer Data that could result in substantial material harm to the Disclosing Party or any of its customers and (iv) ensure the proper disposal of such Customer Data. The Disclosing Party shall maintain reasonable security for its own systems, servers, and communications links as is reasonably designed to (a) protect the security and integrity of its Customer Data to the extent within the Disclosing Party's control, and (b) protect against unauthorized access to or use of the Receiving Party's systems and servers on which Customer Data of the Disclosing Party is stored to the extent within the Disclosing Party's control. The Receiving Party will (1) take appropriate action to address any incident of unauthorized access to Customer Data of the Disclosing Party and (2) notify the Disclosing Party as soon as possible of any incident of unauthorized access to Customer Data and any other breach in the Receiving Party's security that materially affects the Disclosing Party or the Disclosing Party's customers. Either party may change its security procedures as commercially reasonable to address operations risks and concerns in compliance with this section's requirements.

Appendix 2: Sample-B "Information Security" Clause

Supplier represents that it currently follows industry best practices to prevent any compromise of its information systems, computer networks, or data files ("Systems") by unauthorized users, viruses, or malicious computer programs which could in turn be

propagated via computer networks, email, magnetic media, or other means to Company. Supplier agrees to immediately give Company notice if the security of its Systems is breached or compromised in any way. Supplier agrees to apply appropriate internal information security practices, including, but not limited to, using • appropriate firewall and anti-virus software; maintaining said countermeasures, operating systems, and other applications with up-to-date virus definitions and security patches; installing and operation security mechanisms in the manner in which they were intended sufficient to ensure the Company will not be impacted nor operations disrupted; and permitting only authorized users access to computer systems, applications, and Retail Link. Supplier specifically agrees to use up-to-date anti-virus tools to remove known viruses and malware from any email message or data transmitted to Company; prevent the transmission of attacks on Company via the network connections between Company and the Supplier; and prevent unauthorized access to Company systems via the Supplier's networks and access codes. In accordance with all applicable laws of the Kenyan and General Data protection regulation on protection of personal information or privacy of individuals, the Supplier agrees to safeguard confidential protected individually identifiable personal information (health, financial, identity) which are received, transmitted, managed, processed, etc. by Supplier and to require subcontractor or agent to meet these same security agreements.