PremiumTrust Bank

Information Security Guideline in Project Management

Classification: Internal
April 2023
Document Number: PTB/ISMS/ISGPM

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.

Table of Contents

1. Purpose, scope, and users

This control applies to all projects, systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to PremiumTrust Bank systems.

2. Information Security in Project Management

It is vitally important that the organization information assets are always protected, and this is no less true when running a project to achieve business change. These guidelines apply to projects that cover the whole spectrum of business operations and are not limited to those with a significant IT involvement.

PremiumTrust Bank maintains an Information Security Management System (ISMS) which complies with the ISO/IEC 27001:2022 international standard. To ensure that this ISMS remains effective on an ongoing basis it is essential that major business changes which are managed as projects address the issue of how information security will be maintained both during the project and once the project has been delivered.

The main stages of the project management process are:

- **Proposal** – a business case is created for the project and submitted to executive management for approval.
- **Planning** – Approved projects will then be initiated, including the formation of the project team, setting of objectives, creation of the project initiation document and initial project planning. These will be passed through the project board for approval.

- **Design and Execution** – The deliverables of the project will then be created by the project team in line with the approved plan. Risks and issues will be managed, and progress reports delivered to the project board.

- **Transition** – Once tested and accepted the project will move into live operation and the benefits begin to be realized.

- **Project Closure** - The project will then be reviewed and formally closed. This happens after a variable period defined by the project board.

The information security considerations of each of these stages are described in this document. These considerations must be considered as part of each, and every project and their implementation will be subject to later internal and external audit.

2.1 Proposal

The project proposal document itself is likely to contain sensitive commercial information and so must be labelled and protected appropriately as part of the ISMS classification scheme. This may place restrictions on the printing of the document and where it is held electronically. Supporting information such as costing, and resource implications must also be protected in the same way.

The contents of the proposal will obviously vary significantly according to the subject area, but the following considerations should be included in the proposal where appropriate:

Significant risks to information security
Any additional project costs involved with maintaining or improving information security e.g., hardware. software, people
Information security benefits are likely to result from the proposal e.g., risk reduction or avoidance.

These aspects must be included at the outset to avoid the situation where information security controls have to be retrofitted after the project, with little or no available budget, or the organization is exposed to an unacceptable level of risk.

2.2 Planning

2.2.1 Information Security Roles and Responsibilities

Whilst information security is everyone's responsibility, there are several key roles within a typical project which have specific information security responsibilities. These are:

Role	Responsibilities
Project Sponsor	• Champion and emphasize the importance of good information security within the project. • Set information security objectives
Project Manager	• Perform project risk assessments for information security. • Select specific controls based on the results of the risk assessments. • Report to the Project Sponsor on breaches
Project Administrator	• Ensure that information security controls within the project are maintained effectively

2.2.2 Information Security Objectives

As part of the planning stage of the project the information security objectives should be set. These may be included in the same section of the Project Initiation Document as other types of objectives and in the same format.

Where possible the objectives should be SMART. An example information security objective might be:

"To ensure no sensitive information regarding the nature of the project's deliverables becomes public knowledge prior to the official launch on 10th February."

Any information security-related constraints, assumptions and dependencies should also be stated in the project initiation document.

2.2.3 Information Security Requirements

Information security requirements are unique for every project or system. When developing requirements, the following should be taken into consideration:

- The type of information/ data involved.
- The required level of protection for the information or assets involved in relation to confidentiality, integrity, and availability.
- Informing users of their duties and responsibilities.
- Authentication, authorization, and access provisioning requirements.
- Compliance with legal, regulatory, and contractual requirements.

2.2.4 Risk Assessment

An effective risk assessment should be carried out at several stages of the project and information security risks should represent a key part of these assessments. This should consider the assets and deliverables of the project, their vulnerabilities, and the threats that they face during the project. These will include threats to their confidentiality, integrity, and availability.

2.2.5 Selection of Controls

Based on the risks that are identified by the risk assessment that require treatment, appropriate controls will be selected by the project manager. These controls may be in the form of policies, procedures, software, or other suitable ways of addressing the risks effectively.

The controls should be documented, and all members of the project team made aware of them and the reasons why they have been put in place. Any more detailed training in the controls should be carried out prior to the project getting underway.

2.3 Design and Execution

The controls that have been put in place as part of the planning stage should ensure that the information security risks are managed, and the objectives achieved. It may be necessary to update any members of the project team that join after the initial training was delivered. Any third parties used as part of the project should also be made aware of the policies and controls that are in place.

Risk management should be a standard item on the agenda of each project meeting and any changes to risks, including the addition of new ones, should be made as soon as they are identified. Any required changes to controls should also be put in place as soon as possible to ensure the continued security of the project's sensitive information.

Any information security breaches within the project should be notified to the project manager as soon as possible. The project manager will then decide what action to take based on the incident's severity, including the escalation of the incident to the project sponsor.

2.4 Transition

The transition of a project into live running is an event that can complicated and stressful and it is important that enough thought is given by the project team to how information security will be maintained during this period of intensive change.

The project must ensure that sufficient testing has been carried out to check that the security controls defined as deliverables of the project work as intended and that adequate training in them has been delivered to the people involved in maintaining them.

If the project is to be implemented in phases, the project manager must ensure that adequate information security controls are in place during each phase and that security is not compromised in the interests of convenience or speed.

Formal signoff that the information security aspects of the project have been successfully delivered should be obtained as part of the transition into ongoing support. The project manager should also consider whether it would be appropriate to engage a suitable third party to conduct an audit of the security aspects of the delivered project.

2.5 Project Closure

Once the project has been implemented and signed off, a project review meeting will be held to discuss the lessons learned during the project. This is an excellent opportunity to raise any information security-related issues that occurred and to define the best way of preventing them in future projects.

Particular areas for discussion should be:

Were the information security objectives complete and accurate?
Were all of the relevant risks identified?
How successfully were security controls applied?
Were there any security breaches during the project and how did they arise?
Was the balance between security and convenience set about, right?

The lessons learned should be documented and any recommended procedural changes incorporated into the project management method for future projects.

3. Conclusion

These guidelines set out the basics of how information security should be considered as part of the overall framework of project management within PremiumTrust Bank. This involves the creation almost of a "mini-ISMS" within the project to ensure that risks are identified and managed using appropriate controls.

The scope and importance of projects will obviously vary, and the degree of control adopted should remain appropriate to the level of risk involved. Remember however that a small project can still require strong information security if the subject of the project is very sensitive.

Only by applying best practice can we ensure that the security of our information remains protected, and the project team can focus on delivering the benefits set out in the business case.