EN

CERRIX Implementation Guidance

Table of contents

1. Introduction

This document describes the implementation guidelines for the CERRIX GRC-tool. The purpose of this document is to prepare clients for the implementation of CERRIX by giving them insight in how the implementation is structured and what documents / items are needed for a proper implementation. The document will describe project setup, configuration, data quality & import, dashboarding & reporting, go-live & support and project-evaluation.
Readers are advised to take the guidelines into consideration when starting the project. If you have any questions about this document or the project, please contact your CERRIX consultant.

2. Project Setup

As a first step it is recommended to create a project plan. The project plan must contain at least:

1. Project objectives: Describe the objectives you would like to reach with the implementation project. It is important to separate implementation objectives from content & governance objectives.
2. Project scope & phasing: Describe the scope of the project in terms of modules to implemented, processes in scope, frameworks in scope, organizational units/departments in scope, etc. Also describe what you would like to implement in each phase of the project.
3. Terms and conditions: Describe all the terms and conditions that need to be fulfilled to properly execute the project.
4. Convention requirements: Describe all the conventions you would like to use in the project. For example: how you would like to describe risks or controls in the system? By doing this you will maintain consistency in terms of data.
5. Communication plan: Describe the necessary communication steps to reach out to all stakeholders regularly. This is needed to promote the project and the adaptation of the system.
6. Milestone planning: Describe the milestones you would like to reach in each phase of the project and give a detailed description of the underlying items to get to the milestone. Also describe the timelines for each item and the person responsible for delivering the items.

As a second step, after the project group has been selected, it is advised to organize a kickoff meeting to formally start the project. In the kickoff meeting the project goals, scope and planning are discussed with the project group. It also recommended that you make an announcement to all stakeholders in your organization that the project is starting.
As a third step, CERRIX will organize training for all project group members to give them insight and a full understanding of the CERRIX tooling. This training also prepares the project group for the configuration phase as they are inspired to think about items that they need to configure.

Important documents/items to have ready in this phase are:

- **Project plan including milestone planning**
- **Project governance implemented**
- **Project group formed**
- **Communication to stakeholders about the project performed**

3. CERRIX Configuration

In this phase of the project several project meetings are organized to build the configuration in the CERRIX production environment. It is recommended that all stakeholders are present in these meetings since it's the heart of the system.

As a first step we will focus on filling the 3 structures of CERRIX (Organization Structure, Business Dimension Structure, Framework Dimension structures). These structures are hierarchical and so you have the option to build multiple layers (it is strongly advised to keep the number of layers to minimum). The structures are:

- Organization Structure: This represents your organizational tree.
- Business Dimension Structure: You are able to create the cross sections of your risk profile. For example, you can create cross sections based on business objectives or processes or systems or projects (in fact every cross section you can think of is possible).
- Framework Dimension structure: You are able to create control frameworks that you use in your organization. CERRIX is also able to import predefined control frameworks, such as: ISO27002, COBIT, NOREA Privacy Control Framework, SWIFT etc.

As a second step we will configure the meta data of the different modules that are in scope of the project. For example, we can get several items from your existing risk policy that we can use, like the risk scoring method, risk conventions, and risk appetite. These will then be configured in CERRIX in the risk module. This way the system becomes customized for your needs.
As a third step, we will work with your designated administrator(s) to configure the user profiles and relate relevant users to these profiles. CERRIX will provide best-practices for defining the user profiles.
As a fourth step all configuration items that have been configured including the reasons why they have been configured that way should be documented in an implementation document.

Important documents/items to have ready in this phase are:

- Organizational structure of your organization
- List of clearly stated Business Objectives
- Risk Management policy
- Process tree
- List of used systems
- List of Control Frameworks used in your organization
- List of employees (future CERRIX users) and roles
- Controls management (execution, testing) governance & procedures
- Implementation document

Once the entire configuration is ready, it should be reviewed by the system owner and project group members. Based on the outcome, we will proceed to the next phase of the project, Data Quality & Import of data.

4. Data Quality & Data Import

In order for the system to be properly adopted by its users, it is important to have consistent data in the system. That's why as a first step it's strongly advised to perform a data quality review on all items that are to be imported into the system before they are imported! The data quality review should consist of checking for correct use of conventions and the completeness of data. As a best practice CERRIX advises to use the following conventions:

Risk description: a risk should always contain an event, a cause, and an effect.
Control description: A control should always contain the 6w model (Who, Why, What/how, When, With what input / output, What if something is not correct.
T**est plan for design & implementation**: A test plan for design should address the following items:

1. Does the control in design mitigate the related risks?
2. Is the control described according to conventions set for controls (see convention control description)?
3. Is the control actually implemented as described at the time of the test (test of 1).

Also the test plan should contain a description of the expected evidence.
Test plan for effectiveness: A test plan should always contain an assessment of chosen quality aspects (timeliness, completeness, integrity) over a period of time based on a at random sample of the population and should contain a description the expected evidence for that test.
The implementation of CERRIX will show both strengths and weaknesses of your risk management system. Once the data quality review is performed and findings out of the review have been resolved we can continue with the preparation of the data imports.
As the next step we prepare the data imports. CERRIX uses several standard import sheets to bulk import items such as risks, controls, actions, incident, etc. To properly fill the import sheets, we first analyse the data of the client versus data that CERRIX needs for the import. Once the gaps have been identified and resolved we can complete the import sheets and import them into CERRIX. After the import the client is able to link the imported risks to the imported controls or vice versa. Also, test plans for the test of design and the test of effectiveness can be created. This is a manual process.

Figuur 4: Risico management proces voor pensioenfondsen.

Important documents/items to have ready in this phase are:

- Risks Sheet
- Controls Sheet
- Control test Plan Sheet
- Actions Sheet
- Incidents Sheet
- All CERRIX import Sheets

Once this phase is complete we can move on to the next phase Dashboarding & Reporting

5. Dashboarding & Reporting

A very important part of the success of the project is that dashboard & reporting requirements meet client needs. As a first step, you will need to identify the dashboard & reporting requirements. There are several criteria that you need to identify to define good dashboards and reporting requirements:

1. What is the goal of the dashboard or report?
2. Who is the target audience?
3. What visual does the audience want to see?
4. What data filters does the audience want to use?
5. What dataset should accompany the visual?

As a second step, based on the identified requirements CERRIX will setup the dashboards in the production environment. CERRIX offers a standard set of reports that are available to all clients. If the client needs customized report's, CERRIX is able to create these reports in Power BI and host these reports in the CERRIX tool. Also, the rights model that is used in CERRIX remains applicable in the Power-BI reports. A second option is that the client can make use of the available APIs to extract data out of CERRIX to their own data warehouse and make the specific reports themselves. Important documents/items to have ready in this phase are:

- Current reports you are using
- Identified dashboard & reporting requirements based on the criteria mentioned above
- Decision whether to use Power-BI In tool or to extract data from the APIs to your own data warehouse

After all items are imported, we can continue to the next phase, the acceptance test.

6. Acceptance Test

As a preparation for the acceptance test, a test script should be made. The test script should cover all functional areas that the client is going to you use in the system. Also, the test script should cover all user profiles (including the rights used in these profiles) that are used by the client in the system. Finally, the test script should also cover all reports and dashboards that have been setup.

Once the test script is ready CERRIX will transfer all data to the acceptance environment to execute the acceptation test. The acceptance environment will be filled with the data from the production environment. As a next step a session is organised for all project members to perform the acceptance test the system according to the test scripts made available to them. It is advised that all members of the project team are present in this acceptance test.

Based on the outcome of this acceptance test, findings will be shared with CERRIX, and adjustments will be made to the production environment if needed. The outcome of the acceptance tests will also be shared with the steering committee together with a recommendation for “go live” made by the project group. The steering committee will then decide if CERRIX is ready for go live. If this decision is positive, it will be announced to all relevant stakeholders. We can then move on to the next phase, which is “going live”.

Important documents/items to have ready in this phase are:

- **Test Scripts**
- **Test Reports**
- **“Go Live” decision**

7. Go live & Support

Before we can actually go live we first have to train the end users of the system. The training can be given by CERRIX consultants or by trainers from the project group (train the trainer principle). The training should be divided in categories depending on what user profile end users have. This improves training efficiency and focuses on what end users should be doing with the system. Also, hands on training materials have to be prepared and handed out during the training to further improve adoption of the system when going live.

As a second step before going live we should setup the support structure of CERRIX. The first line of support will be provided by the client (IE: Application manager (User management) & Risk managers (For content questions). The second line of support will be provided by CERRIX.

A go live date is determined by the project group in cooperation with the steering committee. Once a go live is set it is strongly advised that support is given to end users after go live for the first iteration of work items in the system. This will strongly improve adaptation of the system.

Important documents/items to have ready in this phase are:

- **Training documentation**
- **Work Instructions**
- **Support Documentation**

8. Evaluation

As the project nears its completion an evaluation session should be organized for all project groups members to evaluate the project. The lessons learnt should be documented to use for further implementation of CERRIX within other business units. CERRIX provides an evaluation form to get further insight in the project results and to further enhance quality of services delivered during projects.

Important documents/items to have ready in this phase are:

- **Documented lessons learned**
- **Filled out a CERRIX evaluation form**