**ANNEX 1**

**Date: …April 2019…………………**

**Engagement Planning Memorandum**

**Audit Engagement: ...IT Audit.................................................**

# Purpose and justification of the engagement

*The implementation of the new SAP-HR ERP-software in the ministry of Economy is due to be completed on the 1st of July 2019. In recent years several smaller and bigger IT-projects in our public sector failed or generated several unforeseen problems (financial, operational, and organizational). The Secretary General of the ministry wants to prevent such failures in the future. The newly to be introduced SAP-system therefore only will be introduced if there is a reasonable level of certainty that this system will deliver what it is supposed to deliver and that potential flaws and risks are mitigated as best as possible. The Secretary General asked the audit department to give additional assurance on these issues as well as on the governance of the implementation-project itself.*

# Description of the activity of the entity and of the audited process

## The audited process

*The SAP-HR system will be introduced by means of a temporary project organization responsible for a flawless implementation. The new SAP-HR system will integrate the following processes: payroll, employee administration, time management, travel management, legal reporting.*

*The project team consists of a project manager, employees from the IT-department and an external SAP-advisor. The Chief Information Officer (CIO) bears the overall responsibility of the project. According to the project-plan, the project is designed according to the governing-principles of Prince-2 (Projects in Control 2).*

*The project of implementation foresees the following stages:*

1. *Assessing current situation;*
2. *Change management plan (+continuity-plan);*
3. *Executing test-phase;*
4. *Transfer moment: going live on July 1st.*

*Key-objectives defined for the transformation towards the new system are:*

*•• Improve the service delivered by the HR department;*

*•• Make better decisions more efficiently (management objective);*

*•• Improve the flow of information among the different departments;*

*•• Modernize the IT platform for HR-processes;*

*•• Single point of entry and information for HR-related data;*

*•• Elimination of manual tasks, fewer mistakes;*

*•• Better processes integration and transparency;*

*•• More productivity and efficiency;*

*•• Lower cost of operating by eliminating obsolete systems.*

# Main risks related to the audited processes

*Typical risks concerned with implementation (and migration towards) similar systems are usually defined with the help of the CIA-triad:* ***C****onfidentially (risk of losing/leaking vital or privacy sensitive information to third parties),* ***I****ntegrity (trustworthiness of the data the system delivers) and* ***A****vailability (continuity, back-up and recovery etc.). In general a sufficient mix of application and general controls should be in place to sufficiently deal with the risks related to the CIA-triad.*

*Other risks are associated with the phase-type approach of the project-structure that should pave the way to a successful implementation of the new system: risks concerning the appropriate governance arrangements of the IT-project itself.*

# Objective(s) and scope of the audit engagement

*The objective of the audit is to give reasonable assurance on the following key audit-questions:*

* *Is the* ***governance*** *of the project designed and functioning in such a way that it will pave the way to successful migration and implementation of SAP-HR within the ministry of Economy?*
* *Is the* ***adequateness*** *of the application- and general controls* ***sufficient*** *related to confidentially of data, integrity of data and the availability of vital information of the HR-related systems during the project phase, migration and delivery phases of the project?*

## *Assurance statements on the proper governance of the project as well as the adequateness of CIA-related controls on application- and general level will be accompanied with recommendations if necessary and applicable. Potential findings and recommendations.*

*The criteria to be used in the audit will be derived from the following audit reference frameworks:*

* ***Prince2:*** *the following Prince2-principles will be leading to assess the proper governance of the project: business case (Continued business justification), defined roles and responsibilities according to Prince2 structure, management by stages (phase-approach including risk management) and focus on products in line with pre-defined tolerance levels. The total norm-set regarding these principles is described in the annex;*
* ***COBIT5:*** *CIA-Triad-criteria will be derived from the following COBIT-5-modules: Align/Plan/Organize (APO), Build/Acquire/Implement (BAI), Deliver/Service/Support (DSS) and Monitor/Evaluate/Assess (MEA). The modules of COBIT5 describe criteria for every stage from planning to fully implementing IT-systems in any type of organization. The crucial criteria per module, as discussed with the CIO, will lead to an assurance statement on the adequacy of the general and application controls at every stage towards implementation;*
* *Existing organizational* ***Procedures and regulations*** *which are relevant for the migration process towards the new SAP-HR system. If these procedures and regulations conflict with requirements of Prince2 and/or COBIT5 it will be noted as an audit finding.*

## Scope

*The audit will not extend its scope by assessing the key-objectives as defined for the transformation towards the new system.*

# Audit methodology

|  |  |  |  |
| --- | --- | --- | --- |
| Audit Objective/question | Key Aspects | Criteria | Methodology(Audit instruments) |
| **Proper Governance:** is the project in line with the Prince-2-principles in design and working at every stage of the project? | Business case | * BC is updated at every stage of project
* The reasons for the project must be consistent with the organizational or program strategy.
* The Project Plan and BC must be aligned.
* The benefits should be clearly identified and justified.
* It should be clear how the benefits will be realized
 |  |
| Roles and responsibilities | * Executive and project management roles are clearly separated
* Etc.
 |  |
| **Sufficient General Controls:** is the overall governance of key IT-processes well controlled/organized in the organization? | COBIT/APO12Manage risks | * A full scope risk assessment regarding the migration to SAP-HR has been conducted;
* The risk paragraph in the planning/design document covers the right issues
* Etc.
 |  |
| **Sufficient Application Controls:** are the controls embedded in the newly to be delivered system (on itself and in conjunction with other systems during the migration phase) sufficient enough to mitigate risks related to the CIA-triad? | COBIT/DSS04Manage Continuity | * Back-up and recovery procedures are implemented in the running software during migration
* Software contains automated provisions in case of disruptions
 |  |

## Audit programme

*This audit-assignment will be conducted in two parallel sets of activities:*

***Activities related to giving reasonable assurance on the governance of the project:*** *the audit-team will conduct real-time audit-activities that timewise are sequential with the project-phases of the audited project. Every phase of the project (4 phases) needs an ‘ok’ from the audit-team before the next phase can start. The audit-team will continuously monitor and assess whether or not the Prince2-principles are adhered to or not. All documents produced by the project will be/can be part of the audit-evidence. Periodically interviews will be held with project-team members, management (CIO) and other relevant stakeholders (e.g. HR-department, IT-department);*

***Activities related to giving reasonable assurance on the sufficiency of general- and application controls:*** *for both the general- and application controls a broad variety of audit techniques will be conducted. E.g. different kinds of test (on application level, pen-testing, security tests, reliability test, integrity tests). Also interviews will be conducted with representatives of the IT-department, HR-departments, policy departments, management (including CIO). Principles of COBIT5 and underlying criteria will serve as reference to formulate our opinion.*

*Both audit-teams will have regularly meetings together to update and inform each other. Both set of activities are considered one audit-assignment.*

**Milestones of the audit:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Project Phase 1(January 2019) | Project Phase 2(July 2019) | Project phase 3(December 2019) | Project phase 4 (July 2020) |
| **Project Audit:**400 hoursx2 team members: 800 hours | Real time+ Go/NoGo after phase+interim report | Real time+ Go/NoGo after phase+interim report | Real time+ Go/NoGo after phase+interin report | Real time+ Go/NoGo after phase+interim report combined with assurance report on controls |
| **General + IT-controls audit**300 hoursx2 team members: 600 hours | Preliminary research | Draft/interim report on design controls in relation to change management plan (APO+BAI) | Draft/Interim report on working of controls during testing phase(DSS+MEA) | Draft/overall report on working of controls during transformation and implemention(DSS+MEA) combined with assurance report on project |

## Resources

*The audit will be conducted in line with the audit charter of the audit department of the ministry of Finance. Information that requires confidentially will be dealt with in line with the provisions made in this charter.*

|  |  |  |
| --- | --- | --- |
| **Role** | **Name** | **Position** |
| Project-leader | experienced ERP-assessor/auditor |  |
| One performance auditor | Prince2-certified |  |
| Two certified IT-auditors | experiences in COBIT-assessments |  |

# Potential difficulties (if applicable)

*A risk for the audit is that the project will be delayed due to unforeseen circumstances. In this case the audit-capacity will be frozen and will be used for other assignments until the project proceeds again.*