**Audit-plan IT-CASE (In Dutch: audit assignment confirmation)**

1. **Preface**

This audit assignment plan describes the audit approach for the ‘Audit implementation SAP-HR’. The described approach is written in line with what was discussed during the intake-phase of the team leader of the audit with the Secretary General of the ministry of Economics.

* 1. **Motive for the Audit**

The implementation of the new SAP-HR ERP-software in the ministry of Economy is due to be completed on the 1st of July 2018. 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.

* 1. **Context**

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.

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.

1. **Assurance Assignment**

**2.1 Client and contractor:**

This assurance-assignment will be conducted by the Audit Department commissioned by the Secretary General of the Ministry of Economy, J.P. Garitte.

Contractor of the assignment is the Head of the Audit Department M. van Kesteren.

This assignment will be conducted according to the International Standards for International Audit (IPPF, 2017) and in line with requirements for assurance assignments as stated by ISACA (assurance standards and guidance for IS-auditors) and NOREA (National Body for IT-Auditors).

**2.2 Objective of the audit**

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.

**2.3 Object of the audit, scope and key-definitions**

The audit will specifically be aimed at the following aspects:

* The project phases as defined in the project-plan. Attention will be paid towards the proper governance of the project-arrangements for each of the defined phases. This means: governance on paper, and the governance how it is actually functioning;
* Application and general controls: related to each phase of the project. This means also the adequateness of controls during the migration/change management phase.

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

Key definitions:

**Proper Governance:** is the project in line with the Prince-2-principles in design and working at every stage of the project?

**Sufficient General Controls:** is the overall governance of key IT-processes well controlled/organized in the organization? This is not related to the project-arrangements but to the functioning of the general governance controls embedded in the organization itself (like the role of the IT-department in relation to the IT-infrastructure, support, change management, logical access controls, authorizations, security);

**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? These controls are on software-level.

**2.4 Criteria**

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.

**2.5 Reporting**

This result of this assignment will be a written assurance report. In this report **reasonable assurance** will be provided on the proper governance of the project and on the sufficiency of application- and general controls.

The assigner/commissioner of the audit, Secretary General J.P. Garitte, is owner of the report.

The report of this audit is primarily intended for the commissioner of the audit (client) with whom this audit (and the approach) was agreed upon. In line with the decision of the Cabinet of Ministers, the ministry that gives the assignment (in the case the ministry of Economy) will publish the report on the web portal of the central government, unless this report qualifies as an exception. The minister of Finance every half year sends an overview of conducted audits to parliament and publishes this list on its website.

1. **Execution of the Audit**

**3.1 Planning and activities**

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 2017) | Project Phase 2  (July 2017) | Project phase 3  (December 2017) | Project phase 4 (July 2018) |
| **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 teammembers: 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 |

* 1. **Team composition**

The audit-team consists of:

* Project-leader: experienced ERP-assessor/auditor: Mr. …….;
* One performance auditor: Prince2-certified. Mrs………;
* Two certified IT-auditors: experiences in COBIT-assessments Mr…… Ms…….

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.

* 1. **Agreements with the contractor/commissioner**

The contractor (in this case delegated contractor: the CIO, auditee) will make sure that the audit team will have access to all relevant information necessary to conduct the audit. The delegated contractor will make arrangements for interviews to be conducted and will announce the audit and its purpose to relevant stakeholders like the project-team, the IT-department and the HR-department. At the end of the audit (foreseen for July 2018) an evaluation of the performed audit-work will be conducted together with the contractor.

Draft reports will first be send and discussed with the delegated contractor (CIO) during each phase of the audit (and the project). Definite (interim) reports will be send to the contractor (Secretary General) and the Audit Committee.

Interviews during the audit will be documented and first be send to the interviewee for comment. Only after approval of the interviewee the interview minutes will be made definite. This also counts for the draft reports and end-report. Each report will be accompanied by a management-reaction.

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.

1. **Signing**

The undersigned agree with this audit assignment and agree with the content of this audit assignment confirmation,

Signed by: team leader and contractor

…………………….

ANNEX: Reference framework / criteria (partly)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Audit Objective/question | Key Aspects | Criteria | Sources | Methodology |
| **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 | Business case  Project documentation | Document study |
| Roles and responsibilities | * Executive and project management roles are clearly separated * Etc. | Project documentation  Project management  Project employees | Document study  Interviews |
| **Sufficient General Controls:** is the overall governance of key IT-processes well controlled/organized in the organization? | COBIT/APO12  Manage 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. | Initiation documents  Project management | Document study  Interviews |
| **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/DSS04  Manage Continuity | * Back-up and recovery procedures are implemented in the running software during migration * Software contains automated provisions in case of disruptions | SAP-HR-system  Old Payroll-system  Old employee administration  Migration documentation | Testing  Interviews  Document-study |