**Case exercise IT-related audit**

The ministry of Economics in country X recently decided to implement a new IT-system aimed at streamlining and automating all the processes related to Human Resource management (SAP-HR). Until now these processes (payroll, employee administration, time management, travel management, legal reporting) were performed by the HR-department of the ministry in a partly automated way, disconnected from each other. In this setting it was very difficult to combine information and/or relate HR-activities with each other. With the new system all this discomfort should be a thing of the past.

The new SAP-HR system should be up and running on July 1st 2018. To achieve this objective a project-team has been assembled with a project manager, employees from the IT-department and an external SAP-advisor. The Secretary General (SG) of the ministry asks the audit-department to perform an audit on the implementation-process of the new system. The SG expressed that the audit department should not only focus on the project itself (is the project in control?) but also give independent and objective assurance and advice on all the intended steps the project-team wants to take (will we achieve the intended objective and really have a reliable, safe and secure SAP-HR system on July 1st?). In addition, the audit department should also be an extra assurance-provider towards (project-) management to make them aware of unforeseen risks. The SG stresses that it is important that the transfer to the new system will be seamless…without a glitch…..without interruption of ongoing HR-processes.

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.

The audit team consists of 4 persons: 1 team leader, 1 performance-auditor, 1 financial auditor, 1 IT-auditor.

**Task:**

Describe the main ingredients for your audit program:

1. What would be the key-objectives of the project? What risks do you see?
2. What would/could be the audit objective?
3. What would/could be the Audit Scope?
4. What will be the general approach for the audit? Techniques? References?
5. What will be the planning and reporting arrangements?

**Additional information:**

The Secretary General agreed and signed the audit plan as discussed earlier. Now the audit team faces the phase of preparing the fieldwork. This means first of all: identifying what specific information the team needs, determine if this information is relevant, have an analysis strategy and determine how the audit process will be documented.

The CIO (delegated contractor) provides the audit-team with the following information:

1. **Information on auditing the governance of the project:**

The CIO stresses that the project evaluation should be focusing on the following PRINCE2 attention points and processes (taking into account the already identified aspects mentioned in the audit plan:

**Main attention points**: Business Case, Organization, Quality, Plans, Risk, Change, Progress.

Processes:

* 1. **Starting Up A Project**, in which the [project team](https://en.wikipedia.org/wiki/Project_team) is appointed including an executive and a [project manager](https://en.wikipedia.org/wiki/Project_manager), and a project brief is produced
  2. **Initiating A Project**, in which the business case is completed and [Project Initiation Documentation](https://en.wikipedia.org/wiki/Project_Initiation_Documentation) assembled
  3. **Directing A Project**, which dictates the ways in which the Project Board oversees the project
  4. **Controlling A Stage**, which dictates how each individual stage should be controlled, including the way in which [work packages](https://en.wikipedia.org/wiki/Work_package) are authorized and distributed
  5. **Managing Product Delivery**, which has the purpose of controlling the link between the Project Manager and the Team Manager(s) by placing formal requirements on accepting, executing and delivering [project work](https://en.wikipedia.org/wiki/Work_(project_management)).[[9]](https://en.wikipedia.org/wiki/PRINCE2#cite_note-9)
  6. [**Managing Stage Boundaries**](https://en.wikipedia.org/wiki/Managing_stage_boundaries), which dictates how to transition from one stage to the next
  7. **Closing the Project**, which covers the formal decommissioning of the project, follow-on actions and evaluation of the benefits.

***Try for each process to think about specific information needs given the attention points and aspects to cover mentioned in the audit plan. Also think about considerations regarding analysis and evaluation.***

1. **Information on assessing the sufficiency of general and application controls:**

**Auditing General Controls**

A general controls review attempts to gain an overall impression of the controls that are present in the environment surrounding the information systems. These include the organizational and administrative structure of the IT function, the existence of policies and procedures for the day-to-day operations, availability of staff and their skills and the overall control environment. It is important for the IT auditor to obtain an understanding of these as they are the foundation on which other controls reside.

A general controls review would also include the infrastructure and environmental controls. A review of the data center or information processing facility should cover the adequacy of air conditioning (temperature, humidity), power supply (uninterruptible power supplies, generators) and smoke detectors/fire suppression systems, a conducive clean and dust free environment, protection from floods and water seepage as well as neat and identifiable electrical and network cabling.

Physical access control is another important area for review. Today in a highly networked world, logical access to computer systems is literally universal, yet there is a necessity to control physical access too. There are certain commands and settings that can be executed only from the console of the server and hence it is important to enclose all servers in a secure location protected by suitable mechanisms like locked doors, access swipe cards, biometric access devices or a combination of these. Further the IT auditors also should review the overall access control measures to the entire facility for controls like security guards at the entry gates, displaying of identification badges and logging visitor access.

**Auditing Application Controls**

Application software is the software that processes business transactions. The application software could be a payroll system, a retail banking system, an inventory system, a billing system or, possibly, an integrated ERP (enterprise resource planning, like SAP-HR) system. It is the application software that understands data with reference to their business context. The rules pertaining to the business processes are implemented in the application software.

Most users interact with the computer systems only through the application software. The application software enables and also limits the actions that a user can do.

It is very important to subject application software to a thorough audit because the business processes and transactions involving money, material and services flow through the application software package.

***Try to determine (based on the chosen reference model (and in this case, common sense) what would be key information that you will need to extract from the business environment? Also think about considerations regarding analysis and evaluation.***