**AUDIT ON IMPLEMENTATION OF SAP/HR**

**WORK PROGRAMME FOR AUDIT FIELDWORK**

| **Nr** | **Process** | **Inherent Risk (before controls)** | **Risk rating** | **Mitigating Controls/Attributes**  **(Expected)** | **Tests of design** | **Control Adequacy** | **Tests of implementation** | **X-Ref**  **Control effectiveness** | **Conclusion** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Confidentially  **DS5 Ensure Systems Security** | Critical and confidential information is not withheld from those who should not have access to it.  Automated business transactions and information exchanges cannot be trusted. | High  High | * *An IT-security plan is defined and maintained;* * *An identity management process is defined, established and it operates;* * *Potential and actual security incidents are monitored;* * *User access rights and privileges are periodically reviewed and validated;* * *The completeness, accuracy, validity and accessibility of stored data is maintained.* * *Technical and procedural controls to protect information flows across networks are implemented and maintained;* * *Vulnerability assessments are periodically conducted* | Establish if there is an IT-security plan;  Review the plans and see if mitigating controls are described  Establish if there if procedures are described related to information flow and data integrity. Review these procedures against the mitigating controls. |  | * Establish the number of incidents due to physical security breaches or failures and the number of incidents of unauthorised access to computer facilities; * Run a PEN-test aimed at testing the mitigating controls that should prevent loss of confidential information; * Interview key specialists which are responsible for the general controls related to confidentiality; * Interview key-users of the system. |  |  |