WORKSHOP 3: Risk management and Information system

Accounting risks

Technical risks

Legal opposition

Accounting risks

Through the exchange axes of the country experiences, the risks related to the accounting function flow:

- ❑ Errors in entering accounting transactions (multiple entries or double entries);
- ❑ The processing of provisional imputation accounts and transfer accounts;
- ❑ Poor bookkeeping in deconcentrated posts;
- ❑ Late or incomplete reporting of accounting data;
- ❑ Errors in budgetary or accounting imputations;
- ❑ Non-control of the transition from cash accounting to accrual accounting in recognized rights and obligations;

Technical risks

Technical risks may be related to:

- a non-robust information system whose architecture does not allow a good integration of equipment and software solutions;
- a periodic failure to audit the information system to detect any vulnerabilities;
- a physical security defect in the data center, physical access control and software;
- poorly defined levels of entitlement;
- bad backup of databases, lack of data replication or backup on a remote site or cloud hosting (recovery plan);
- poorly implemented or anomalous accounting functions;
- a lack of documentation to ensure the continuity of the service (assignment of personnel);
- the lack of control over the confidentiality and integrity of the data;

Legal opposition

Dematerialisation involves technical and operational but also legal aspects relating to opposability, namely the legal value of dematerialized budget and accounting acts. It is:

- ❑ The legal value of supporting documents for budgetary and accounting transactions, in particular invoices and contracts or dematerialised public contracts;
- ❑ The opposability and legal value of the electronic signature;
- ❑ Generating facts to keep in the database (electronic filing of documents);
- ❑ The acceptance of the data generated by the information system by the auditor.

Recommendations (1/2)

Some recommendations to take into account:

- ❑ Encourage the implementation of integrated budget and accounting management systems;
- ❑ Develop physical security plans and information system software;
- ❑ Adopt a rigorous authorisation policy (access rights) to be monitored by a control and internal audit system;
- ❑ Establish internal control: mutual control or validation and supervision including data entry;
- ❑ Establish computerized and automated "on-board" controls;

Recommendations (2/2)

- Agreeing standards and processes with the Court of Auditors as soon as the information system is designed (validity of vouchers and dematerialised invoices);
- Ensure the coverage of all Treasury business and all stakeholders by the information system adopted;
- Have software for analyzing or auditing the information system;
- Create a legal framework for the validity of the electronic signature and the protection of personal data;
- Agree with the Court of Auditors on the inclusion in the determination of the result of the accounts of provisional allocation of expenditure relating to advances to the budget; which makes it possible to regularise the accounts of provisional imputation of expenses in management n + 1.