

Internal control and deontology

Chapter 7: IT auditing

1. Risks and opportunities

- Risks:

- (-) less oral communication and personal contacts □ errors, misunderstandings, ... could arise and exist longer
- (-) fewer formal registrations
- (-) small programming errors are repeated frequently thus resulting in large errors

- Opportunities

- (+) time savings and more efficiency
- (+) basic controls and checks can be programmed
- (+) LOG files
- (+) faster, better (more efficient) management reporting is possible (dashboards, mgt cockpits, etc)

Attention!:

- ✓ Don't forget: reliability of output depends on input ("*garbage in = garbage out*")
- ✓ Segregation of duties is crucial

2. I/C in an IT environment

Specific internal control aspects:

Responsibilities:

- Who is responsible for the design, development, (testing), implementation and maintenance of the IT systems? □ the **IT department**
- Segregation of duties is important:
 - Implementation, testing, approval of new systems
 - Creation of user ID's and passwords
- Otherwise: same principles as in a non-automized environment
- IT department should never make changes/alter the system without permission (unilateral)

- Security:
 - Physical security: fire, floods, inappropriate access,
 - Technical security: use of passwords, pincodes, etc.
 - What is a good password?:
 - ✓ passwords are personal
 - ✓ Frequently changed
 - ✓ complex (special signs)
 - ✓ Kept in a safe place
 - ✓ Automatic logging of (attempted) access to personal data
 - Security is not a one time effort!
 - ✓ logging and keeping track of access attempts
 - ✓ Privacy policy
 - ✓ Only using legal software versions
 - ✓ Contingency planning– continuity – reputational damage

3. CAAT's

- Computer Assisted Audit Techniques:
 - Specific audit software (ACL, Idea, ...): more powerfull than Excel
 - Usefull for:
 - ✓ retrieving double payments
 - ✓ Retrieving 'gaps' in data
 - ✓ Linking databases
 - ✓ sampling