Digital Forensics

Marian Svetlik

svetlik@df-pro.cz

svetlik@fi.muni.cz

www.digital-forensic.pro

MUNI

# Digital Forensics Course Concept

MUNI

Marian Svetlik

- Expert Witness in Digital Forensics
- Information Security Expert
- Vice-president a CEO of The Academy of Forensic Sciences
- Digital Forensic Review - Journal Editor
- ISMS Lector at University of Economics Prague
- Comuter Crime Lector at University of Finance and Administration Prague
- Cybercrime Lector at CEVRO Institute
- Digital Forensic Special Expert C4e at MUNI
- Programme Committee member of the DFRWS EU
- IDFA Management Board Member

Course Content

- DF definition, relation to the cybersecurity and to the cybercrime
- Digital Traces & Digital Evidence, properties, documentation
- Sources, Handling, Gathering and Protection
- DF Examination Principles
- DF Lab creation and management, Assessment, Certification, Accreditation
- DF in Law, Electronic Evidence

Recap

- Digital Forensics Examination Models
  - Preparation; Identification; Collection/seizing; Integrity; Examination; Analysis; Reporting; Presentation; Archiving/deleting/returning
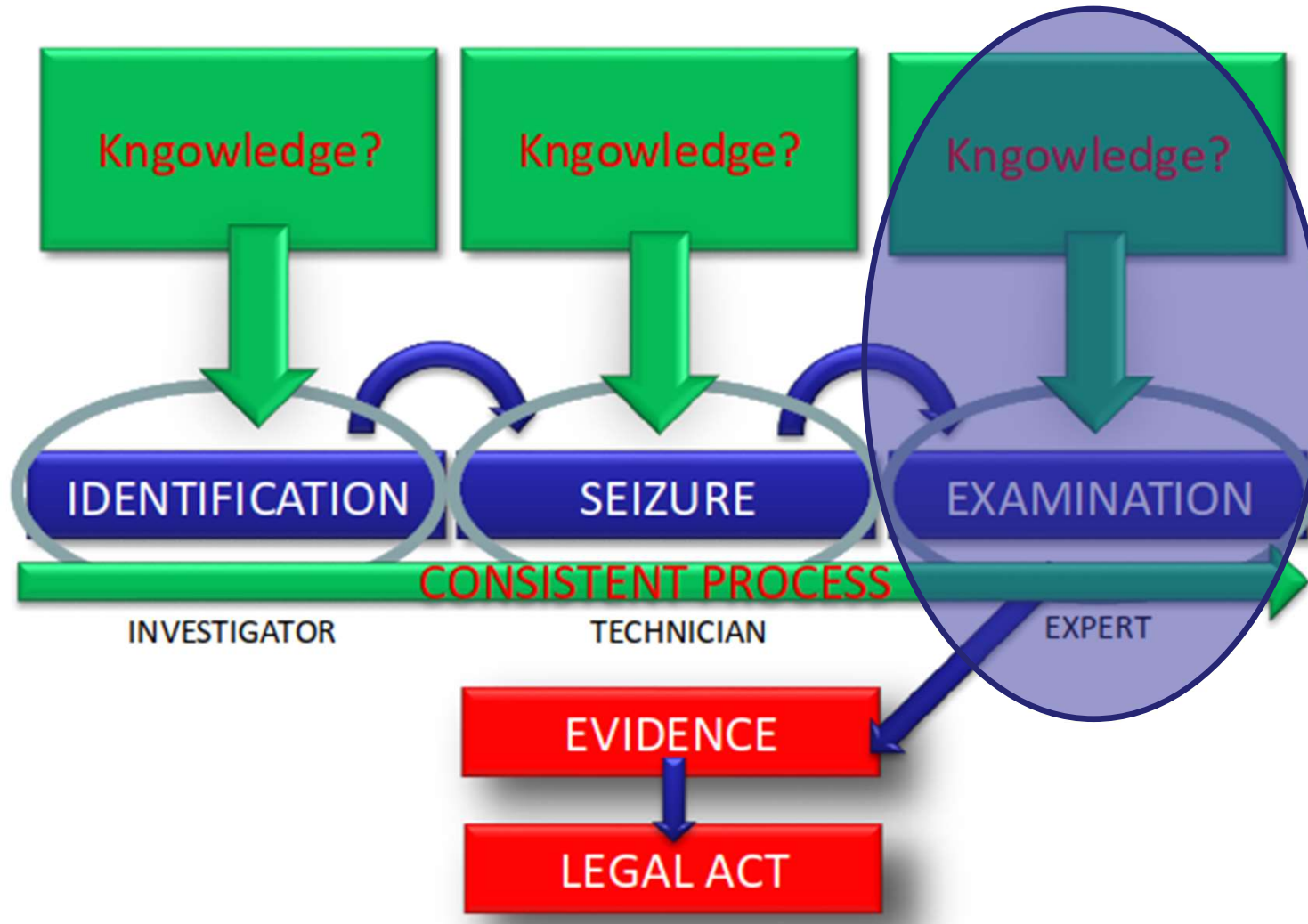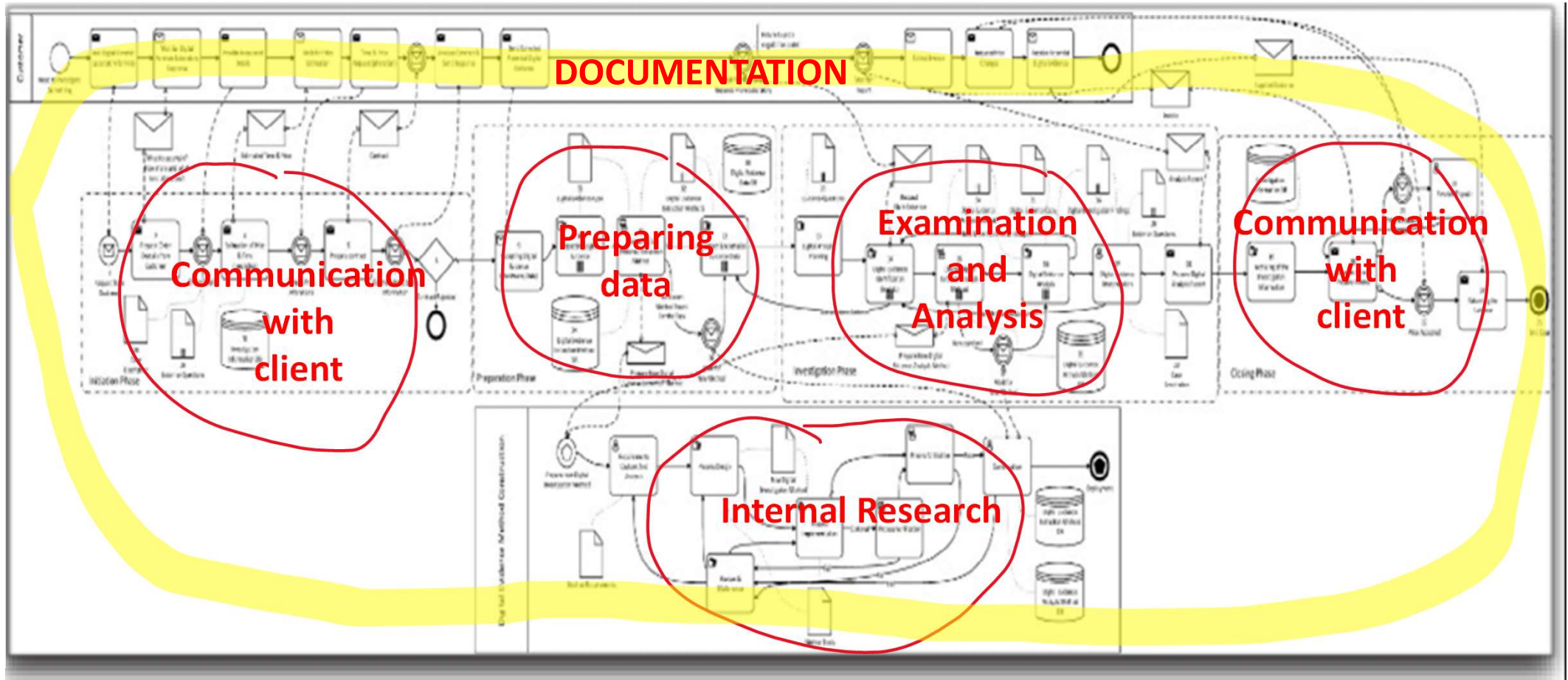
Recap

MUNI
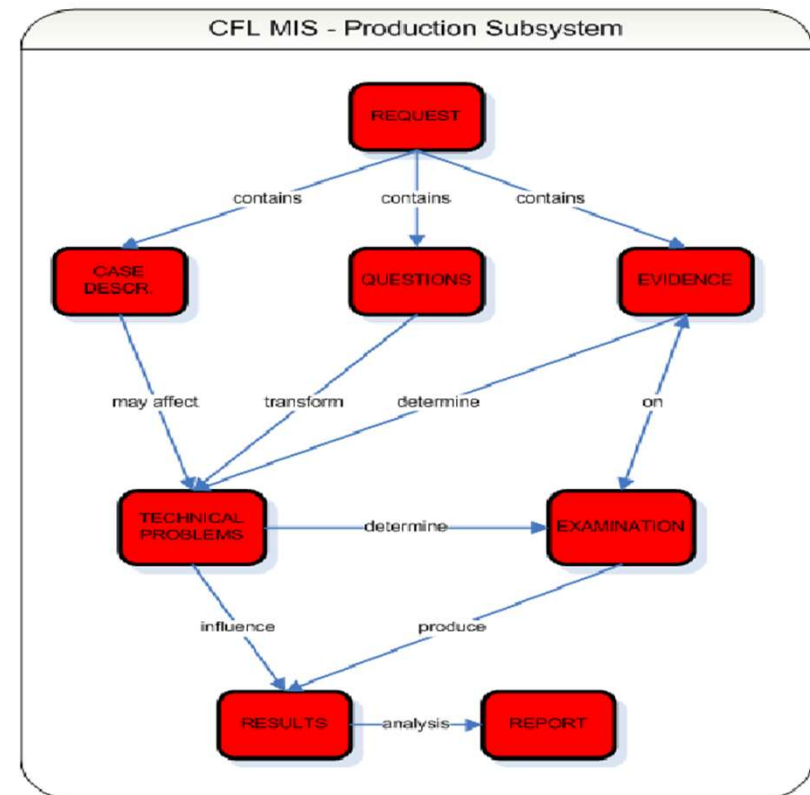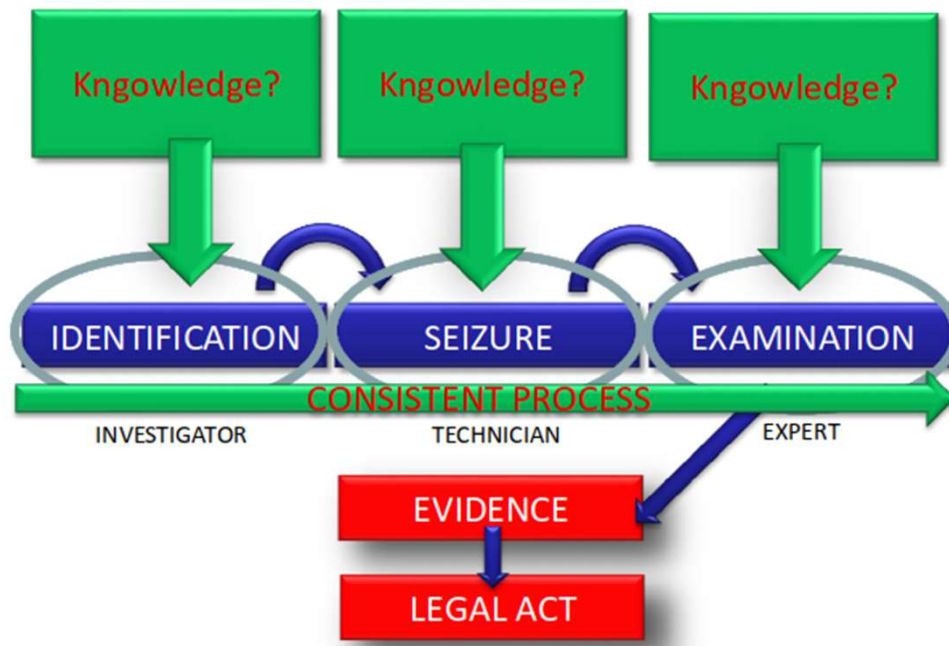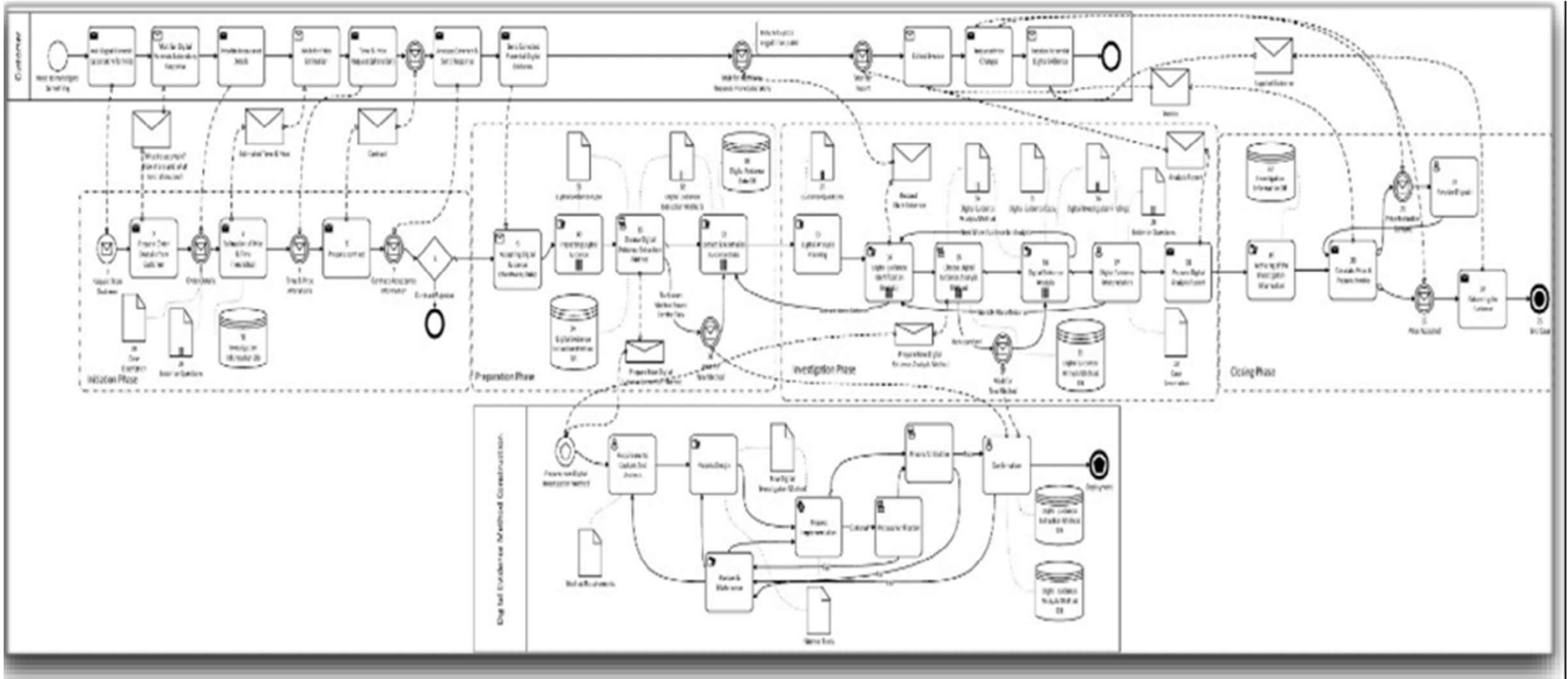
Today outline

Digital Forensics Laboratory:
building
managing
certification and accreditation

MUNI

Examination

MUNI

Process

Creating DF Lab

- **Why?**
  - Reasons
  - Position
  - Goals
  - Competency
  - Effectiveness
  - ...

DF Lab Process Model
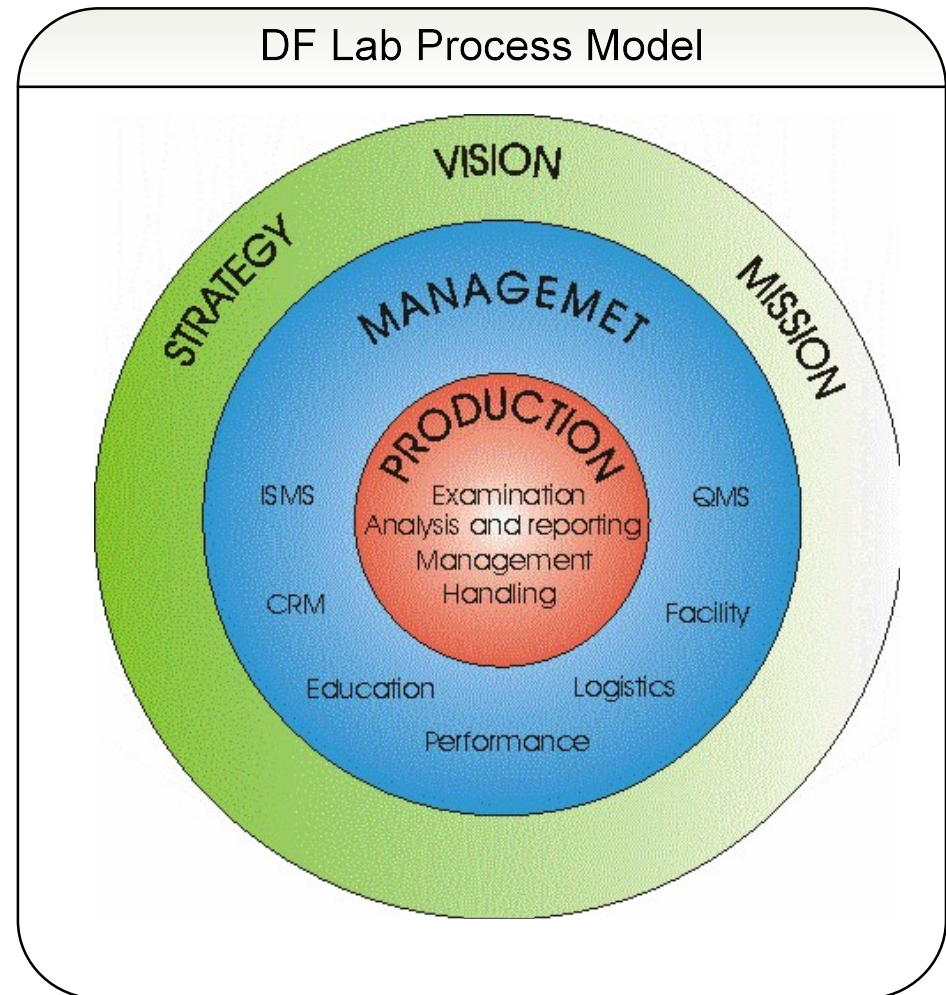
What we will need?

- Management support
- Budget (starting as a min at 1M CZK ~ 40 000 EUR) /year/person
- Managing creator

MUNI

What we will need (1)

- People (with screening)
  - Manager (1)
  - Assistent (1)
  - Analyst(>1)
  - Expert (>1)
  - Technician (>1)
  - Purchase officer ? (1)

What we will need (2)

- Office (ground floor/freight elevator) physically secured
  - Open part
    - Entrance space
    - Assistant office
    - Meeting/presentation room
  - Cosed part
    - Documentation space
    - Delaboration space
    - Duplicating space
    - Analysing space
    - Reporting space
    - Case storage space
    - Archiving space

MUNI

What we will need (3)

- Technology (HW &SW) most of them non-standard
  - Computing power
  - Big and quick storage
  - Dedicated separated high-speed network
  - Special forensic HW & SW tools
  - Store of spare parts
  - Forensic lab/case management SW

What we will need (4)

- Special docomentation tools
  - Permanent (at lab) (separate or linked up system)
    - Photo
    - Video
    - Voice
    - Lighting (with enough space and backdrop)
  - Portable version (at crime scene)
  - Special (criminalstic) – secure tapes and labels, fixs, numbers, measures, seals, …

What we will need (5)

- Portable equipment (various cases in „Pelican" design)
  - Documentary case
  - Data duplication case
  - Tool case
  - Notebook &printer case
  - Administrative (brief) case

What we will need (6)

- ?

DFLab certification

- Local(?) government certificate
- Reliable (local?) association certificate
- ISO/IEC 17025 certification (17020, 2700x)

MUNI

MUNI