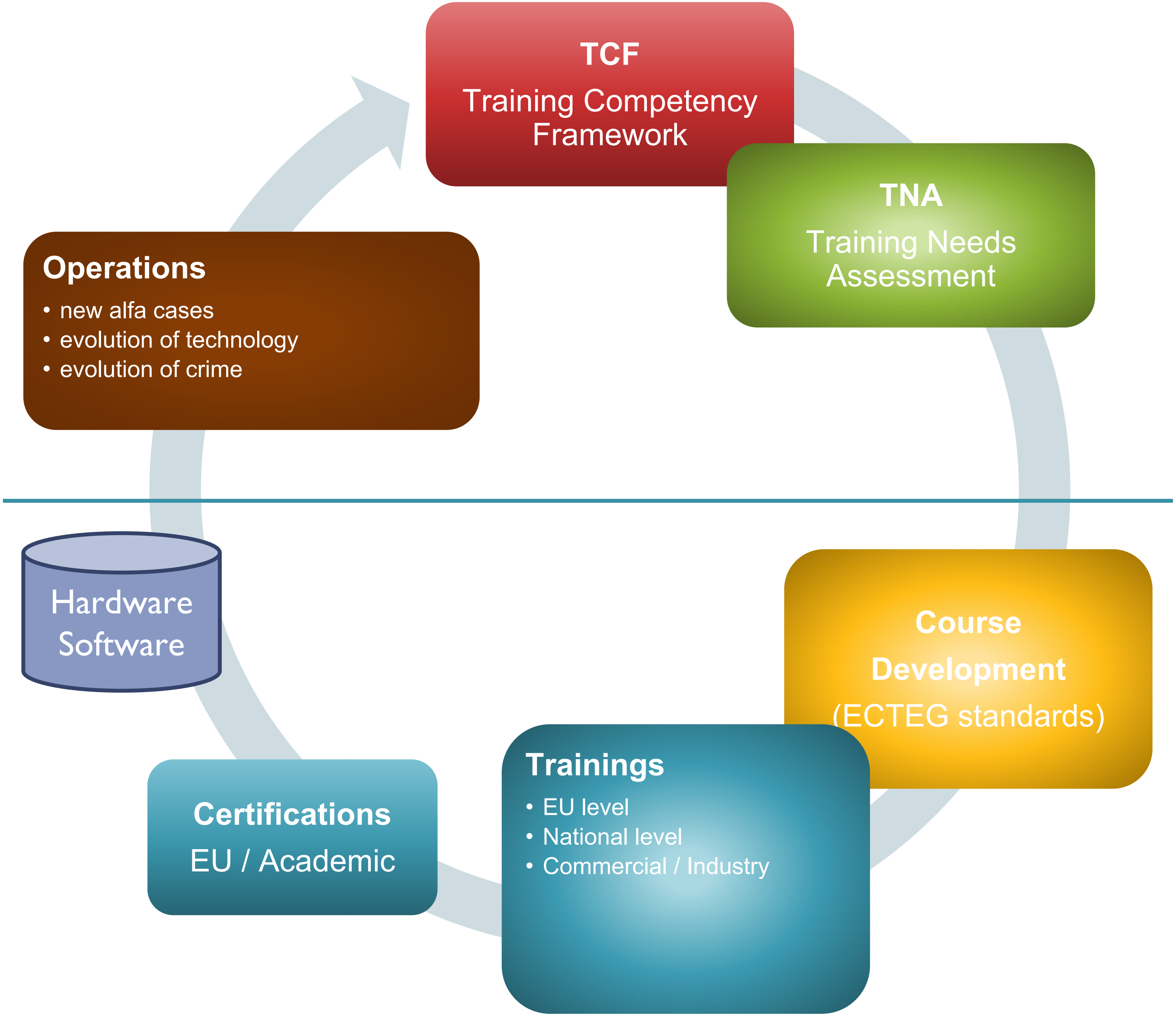
E.C.T.E.G.

Yves Vandermeer
MSC Computer Forensics and Cybercrime Investigations
PhD researcher
Detective Chief Inspector - FCCU - Belgium
E.C.T.E.G. chair

yves.vandermeer@ecteg.eu



TCF

Training Competency Framework

TNA

Training Needs Assessment

Course Development

(ECTEG standards)

Trainings

- EU level
- National level
- Commercial / Industry

Certifications

EU / Academic

Operations

- new alfa cases
- evolution of technology
- evolution of crime

Hardware
Software

EUROPEAN CYBERCRIME TRAINING & EDUCATION GROUP
E.C.T.E.G

Training Competency Framework

Matrix of Required Knowledge and Skills for LE Actors

	Management Skills				Technical Skills					Investigation Skills					
Discussed Category	Strategic Decision Making	Management (incl. HR & Budget)	Soft Skills and Networking	Communication (incl. presentation)	Digital Forensic Skills	Internet Networking & Tracing	Programming, scripting, SQL	Analytical & Visualisation Skills	Live Data Forensics	Cybercrime Legal Knowledge	General Cybercrime Awareness	First Responder Training	Open Source Intelligence	Interviewing & Interrogation	Investigation Techniques
Political and Strategic Decision Makers	■	■	■	■						▨	▨				
Law Enforcement Management	■	■	■	■						■	▨				
Heads of Cybercrime Units and Team Leaders	▨	■	■	■		▨				■	■		▨		▨
General Criminal Investigators				▨		▨				▨	▨	■	▨	■	■
Intermediate and Advanced Investigators				▨		▨				▨	▨	■	▨	■	■
Cybercrime Analysts and Intelligence Officers				▨	▨	▨	▨	■		▨	■		■		■
Online Investigators				▨	▨	■	▨	▨	▨	■	■	▨	■	▨	■
Digital Forensic Investigators and Examiners				▨	■	▨	▨	▨	■	■	■	■	▨		■

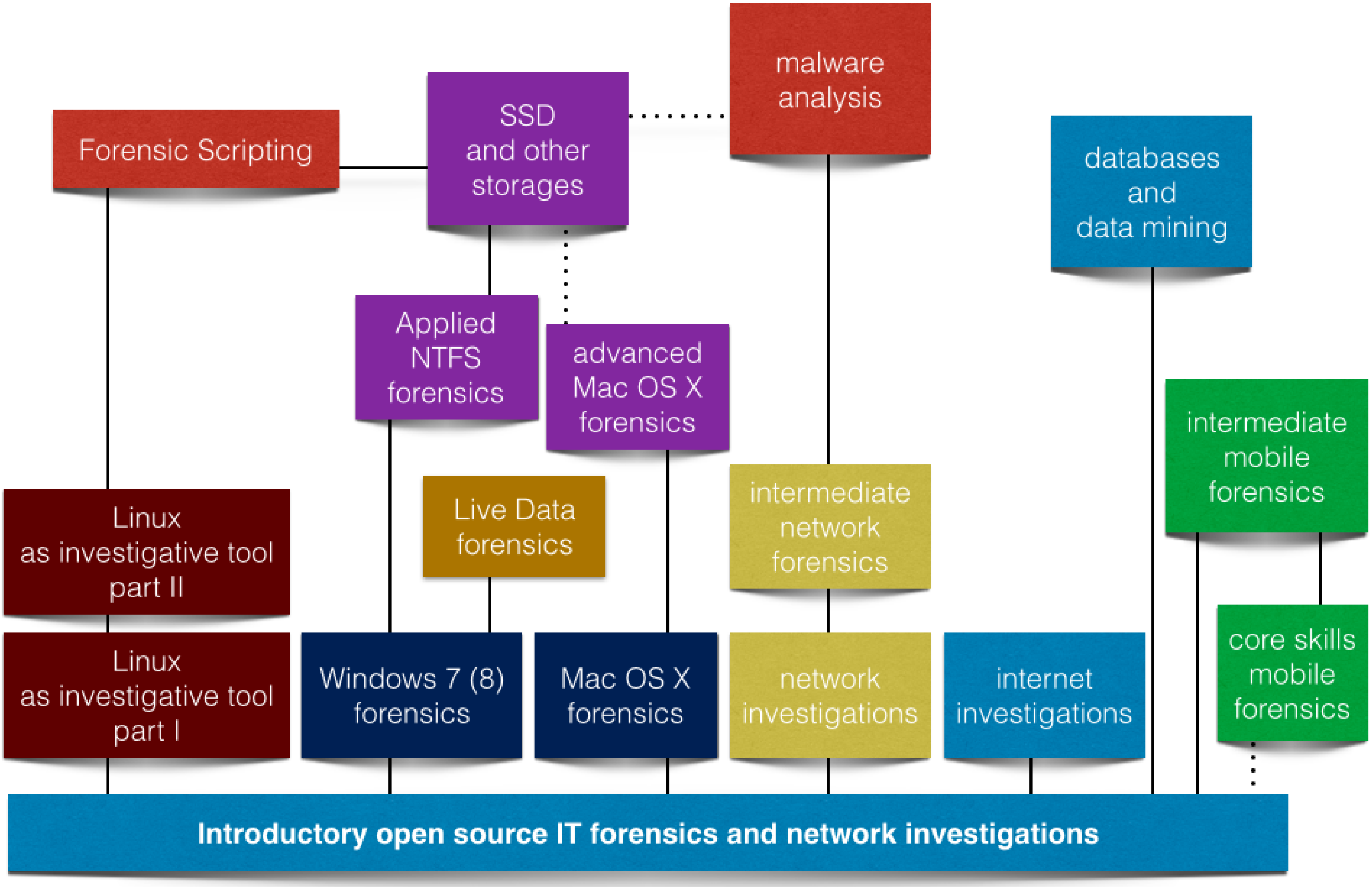
Relevant Cybercrime Training

Requirements

▨ Basic level

■ Expert level

ECTEG training packages



Forensic Scripting

SSD and other storages

malware analysis

databases and data mining

Applied NTFS forensics

advanced Mac OS X forensics

intermediate mobile forensics

Live Data forensics

intermediate network forensics

Linux as investigative tool part II

Linux as investigative tool part I

Windows 7 (8) forensics

Mac OS X forensics

network investigations

internet investigations

core skills mobile forensics

Introductory open source IT forensics and network investigations

E.C.T.E.G. standards

- Focusing on the TCF profiles
  - To know
  - To do
  - To be able to explain in front of court

E.C.T.E.G. courses materials

- Includes :
  - Trainers manual
  - Students manual
  - Presentations
  - Exercises ands tools
- Available for :
  - LEA only
  - Free of charge

The digital evidence exception

- Difference between technical evidence and expert evidence ?
  - Live data forensics needs to take decisions
  - Chip-of is sometimes destructive
  - Cloud storage and IoT challenges
  - Cyber attacks and networks
- Reproducibility is not possible anymore
- Traces without interpretation are often useless
- How many DF certified labs ?

Way to practitioners certification

“good practices” can be defined and have to be frequently updated.

We have to work on how good practices are applied :

- dissemination and training
- assessing practitioners
  - competences
  - skills

Certification model

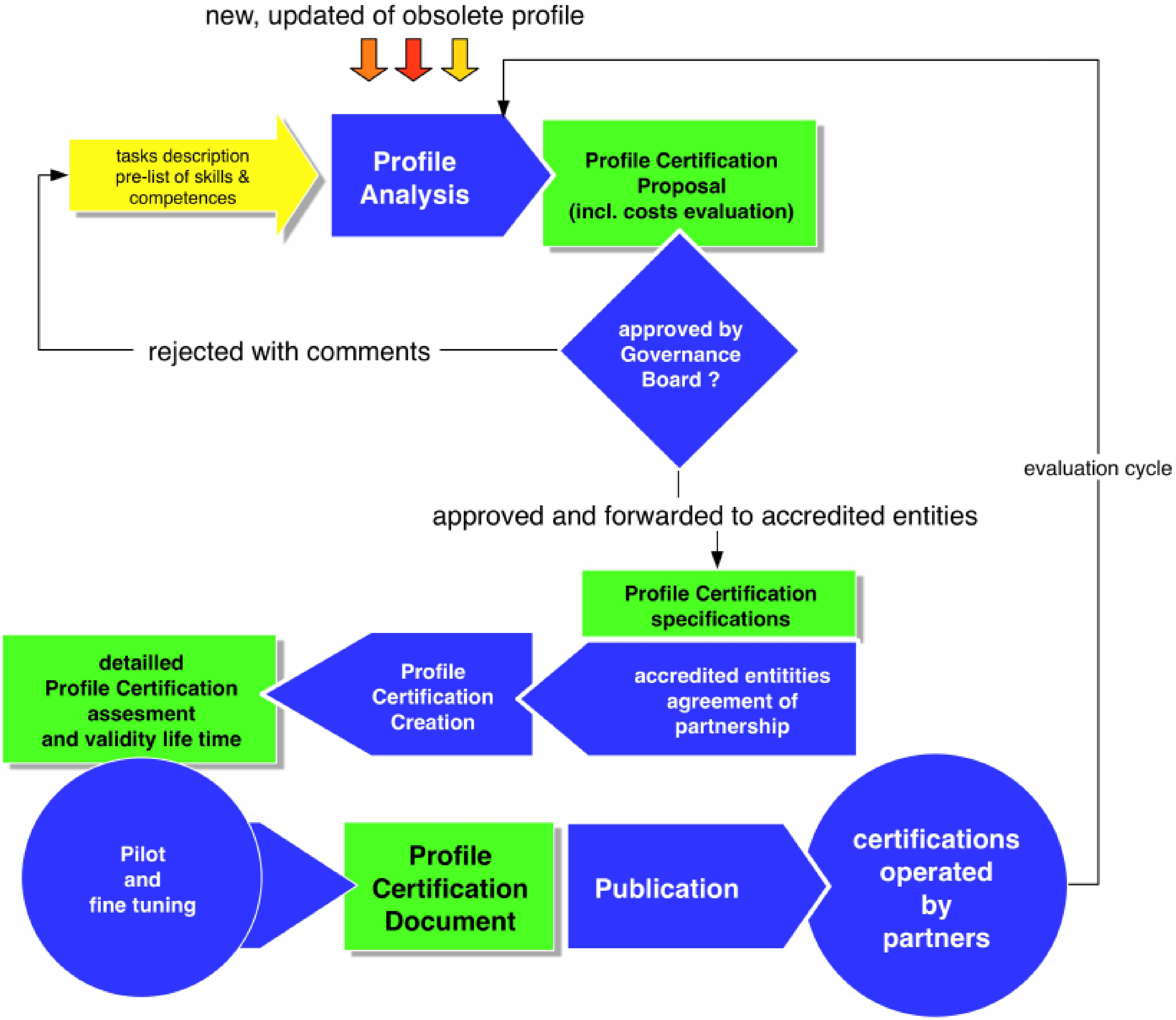
Carlota Urruela

Universidad Autónoma de Madrid

carlota.urruela@uam.es

Practitioners certification model

- Profile based certification
  Using Training Competency Framework as backbone
- Unlinked from the training (neutral)
- Checking competences and skills
  - Theory & practice by academic partners
  - Internship for some profiles (i.e. softskills)
- Limited validity 5 ≃ 2 years
- Transition path from exiting ones
- Compatible with academic degrees (bachelor, master)
- Model created by TOT project (2015-2016)
  - Prosecutors, investigator judges, law enforcement, academics
  - Support from Europol, Eurojust and ECTEG



new, updated of obsolete profile

tasks description
pre-list of skills &
competences

Profile
Analysis

Profile Certification
Proposal
(incl. costs evaluation)

approved by
Governance
Board ?

rejected with comments

approved and forwarded to accredited entities

Profile Certification
specifications

accredited entitities
agreement of
partnership

Profile
Certification
Creation

detailled
Profile Certification
assesment
and validity life time

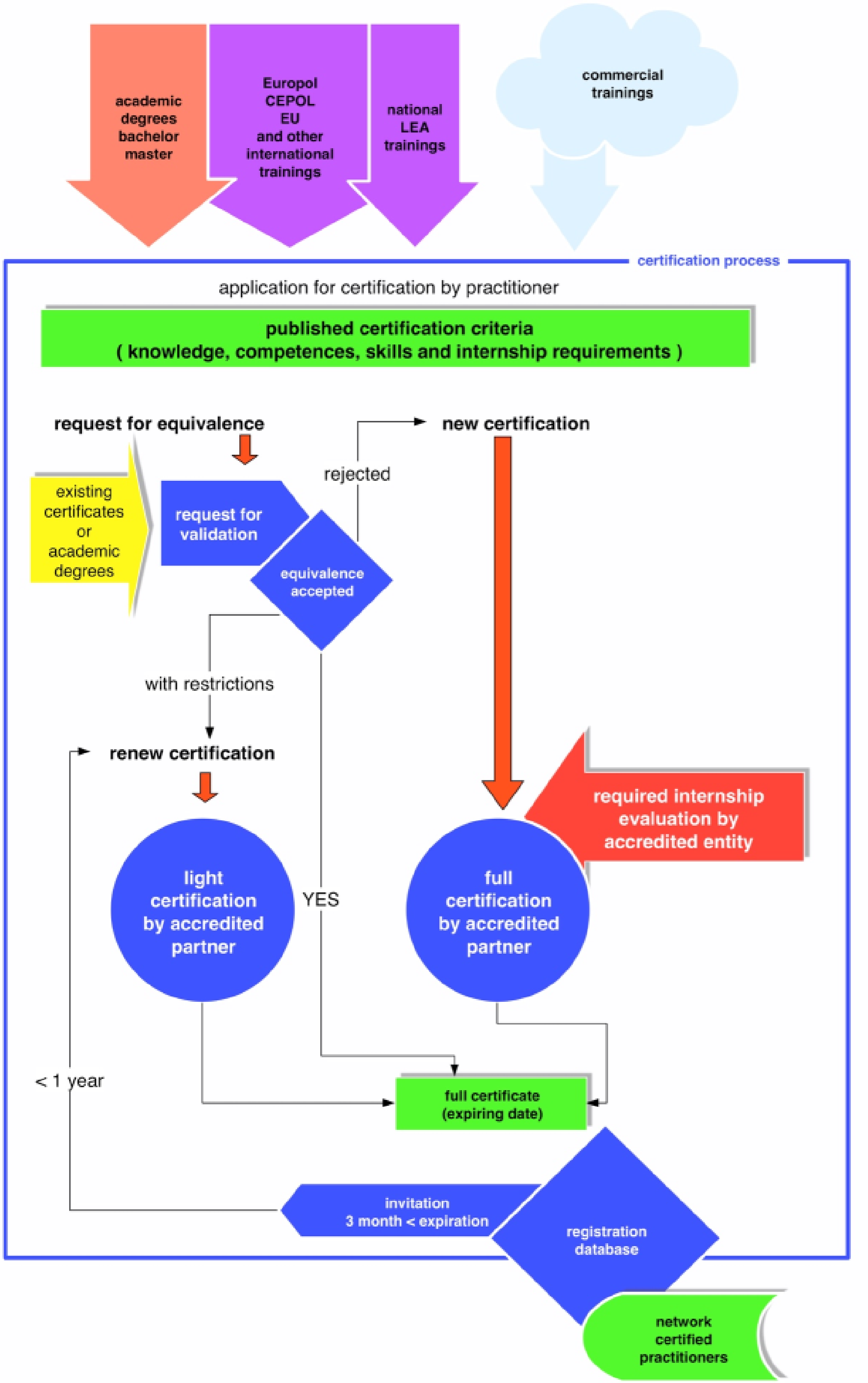
Pilot
and
fine tuning

Profile
Certification
Document

Publication

certifications
operated
by
partners

evaluation cycle



academic degrees bachelor master

Europol CEPOL EU and other international trainings

national LEA trainings

commercial trainings

certification process

application for certification by practitioner

published certification criteria
(knowledge, competences, skills and internship requirements)

request for equivalence

existing certificates or academic degrees

request for validation

equivalence accepted

rejected

new certification

with restrictions

renew certification

light certification by accredited partner

YES

full certification by accredited partner

required internship evaluation by accredited entity

< 1 year

full certificate (expiring date)

invitation 3 month < expiration

registration database

network certified practitioners

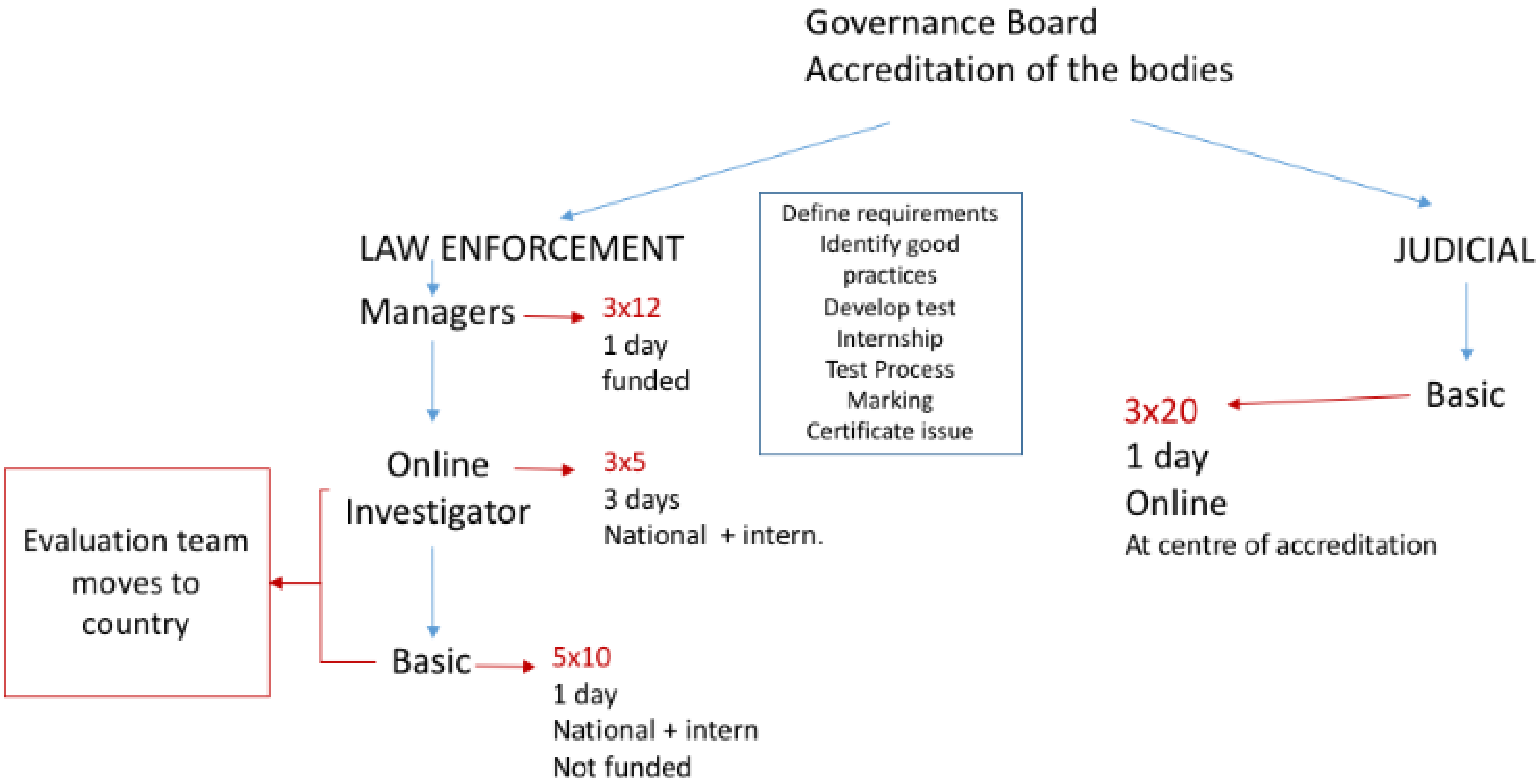
- Need to check certification quality

- Equipment defined by profile

Step forward –implementation

- Already advised when
  - Creating new profiles
  - Creating new training packages (CyberEX project)
- Governance board
  - Europol, CEPOL, Eurojust, ECTEG, EUCTF, EJTN
- Accreditation by
  - Accreditation of members
  - Checking implementation by member
- Certification database

Project Proposal



Governance Board
Accreditation of the bodies

LAW ENFORCEMENT

Managers

3x12
1 day
funded

Online Investigator

3x5
3 days
National + intern.

Basic

5x10
1 day
National + intern
Not funded

Evaluation team moves to country

Define requirements
Identify good practices
Develop test
Internship
Test Process
Marking
Certificate issue

JUDICIAL

Basic

3x20
1 day
Online
At centre of accreditation

EUROPEAN CYBERCRIME TRAINING & EDUCATION GROUP

E.C.T.E.G

Way to a (new) ecosystem

- Standard Operation Procedures
  - *ISO/IEC 27037 (2012)*
  - *ENFSI - BPM for the Forensic Examination of Digital Technology (2015)*
  - *ACPO - Good Practice Guide For Digital Evidence (2014)*
  - *Council Of Europe - Electronic Evidence Guide 2.0 (2014)*
  - *ENISA - Strategies for incident Response and Cyber Crisis cooperation (2016)*
  - *S.D. Brown - Investigating and Prosecuting Cyber Crime (2015)*
- Tools
  - features taxonomy from "EVIDENCE" project (*2016*) http://wp4.evidenceproject.eu/dft.catalogue/dftc.home.php
  - FREETOOL project (I & II)
- Practitioner career path within profiles matrix
  TCF by EC3, ECTEG and CEPOL (2015)
- Course packages coherent and structured
  ECTEG 2.0 – Training Needs Assessment Process
- Practitioners certification procedures
  TOT project - *Universidad Autónoma de Madrid (2016)*