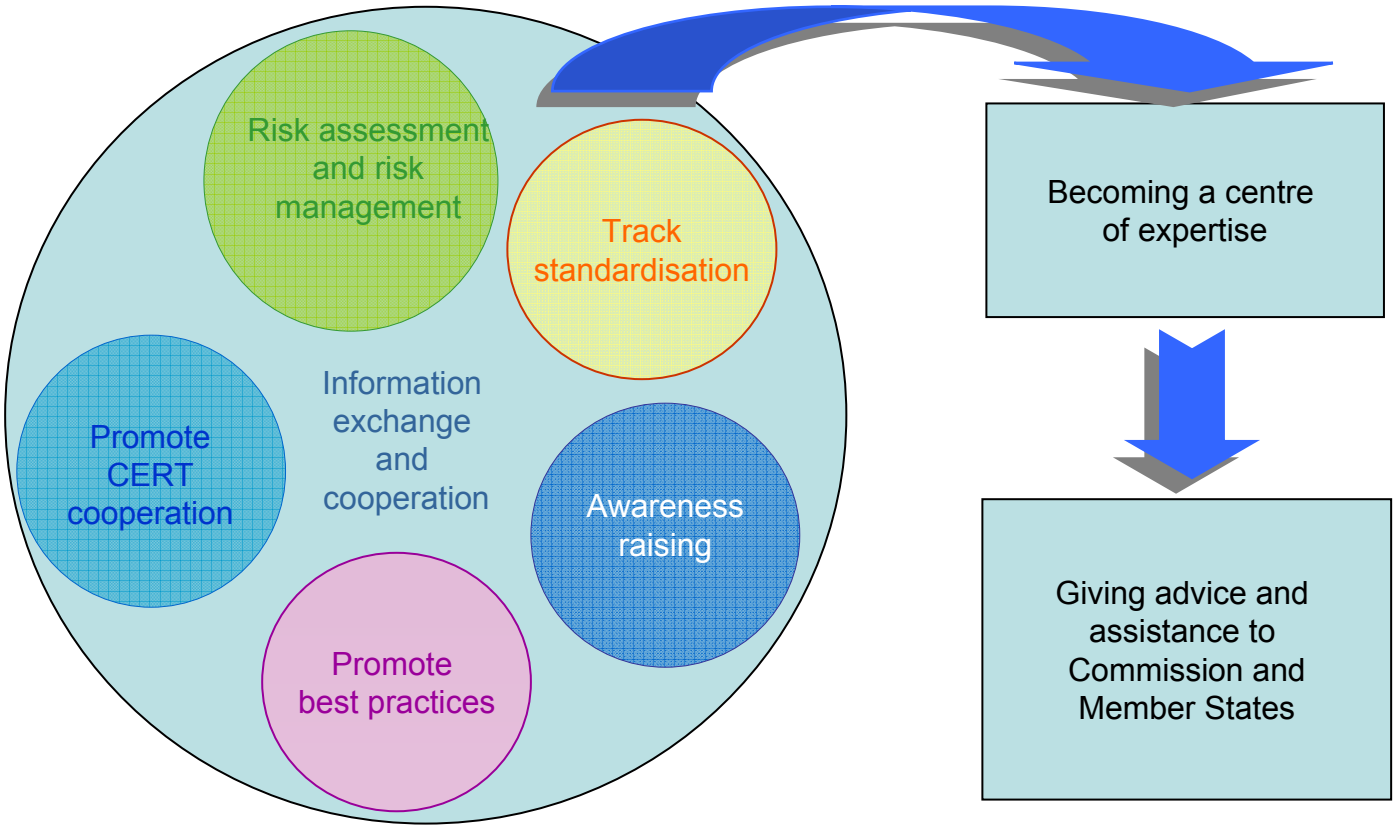
EU initiatives on network information security

Dr. Andreas Mitrakas
European Network & Information Security Agency (ENISA)
Electronic Communications Security event
Athens, 1June 2006

Agenda

- Information Security Considerations
- Business drivers of information security
- EU legal framework
- International Background
- Standards
- The Member States' viewpoint

Tasks of ENISA



EQ: ENISA Quarterly

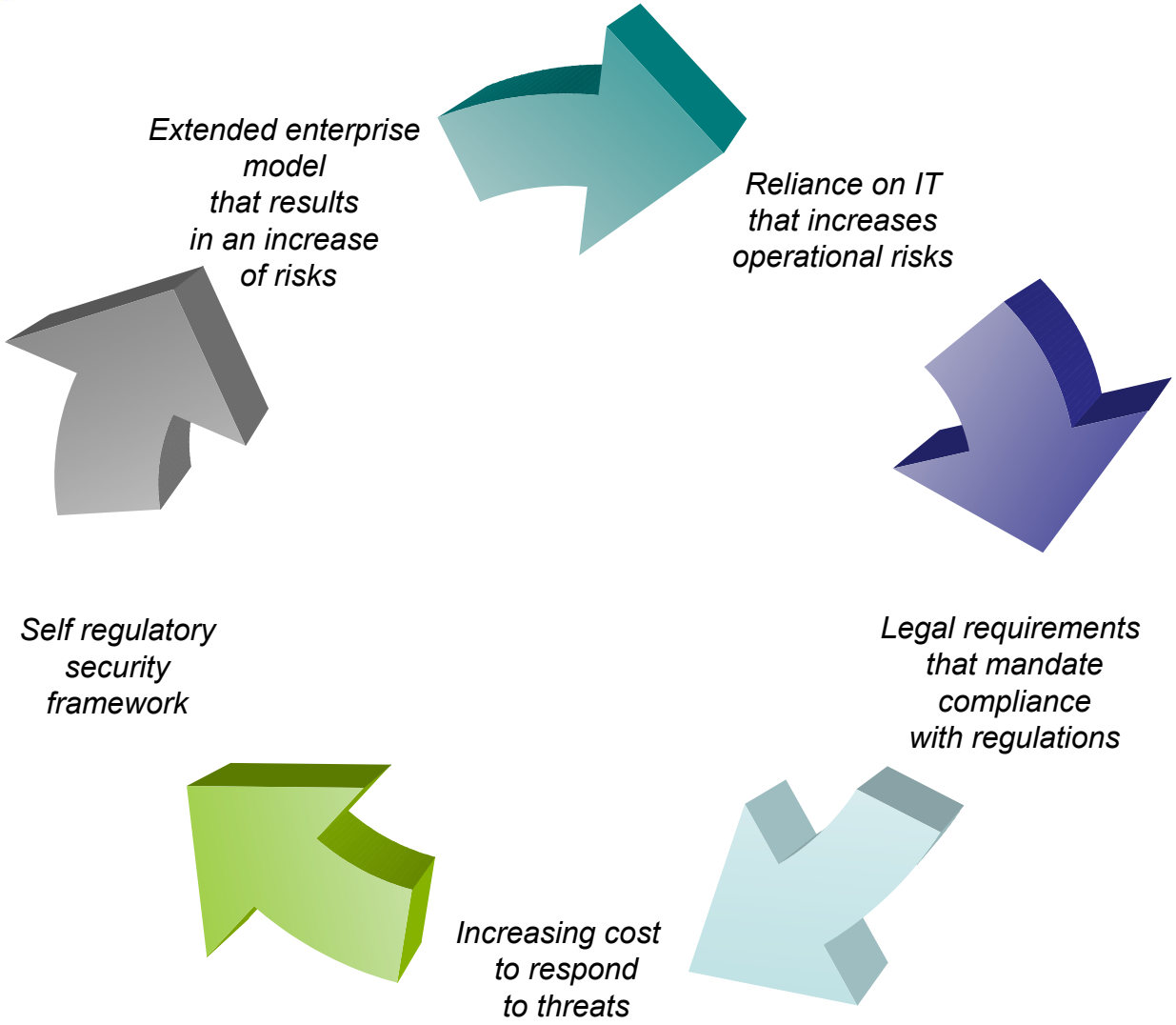
FREE subscriptions to the EQ

http://www.enisa.eu.int/publications/index_en.htm

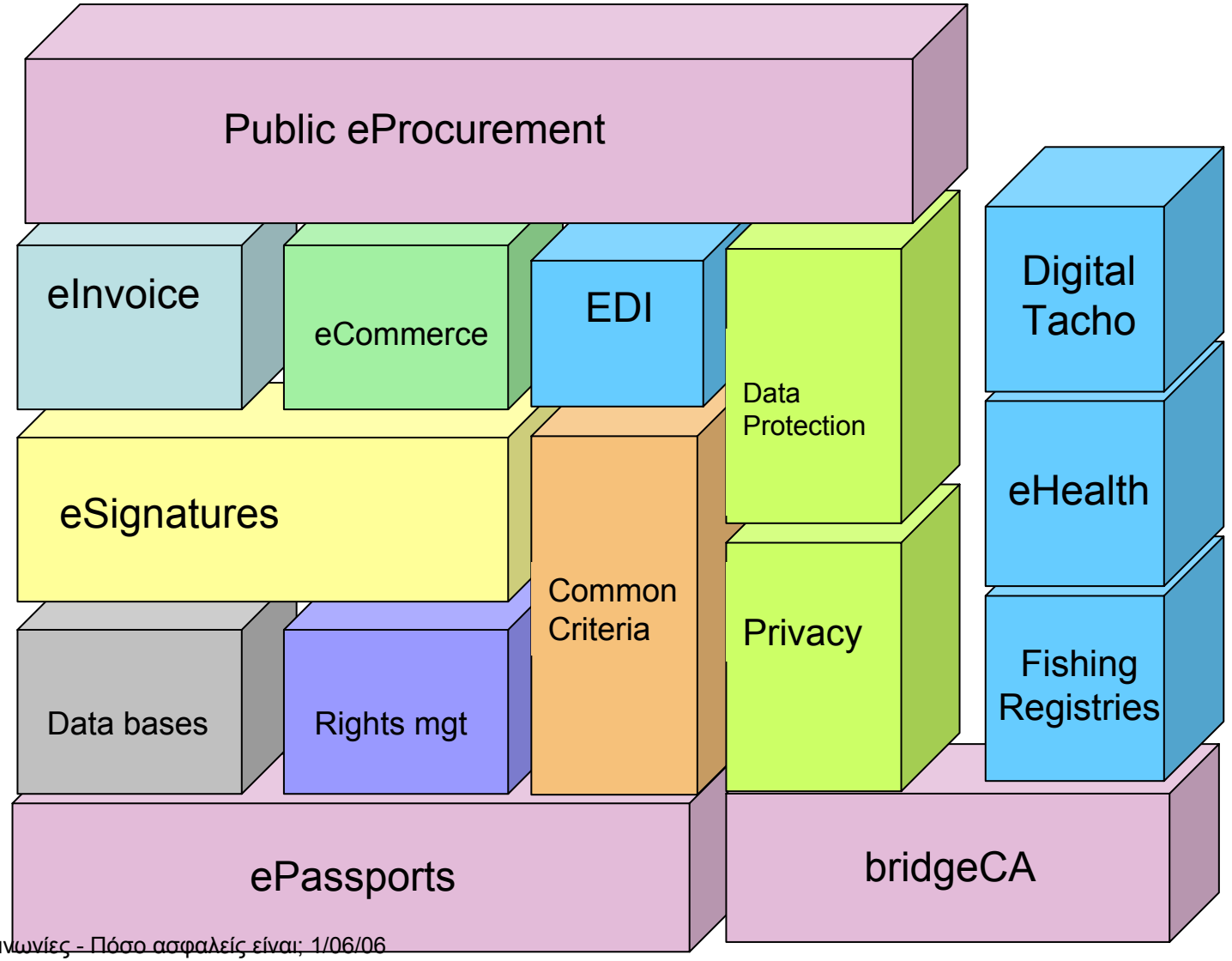
Why Security?

- Security as a means to protect legal rights
- Confidentiality / trade secrets
  - Health care, justice, business transactions
- Prevention of fraud /cybercrime
- Accountability and apportionment of responsibility
  - Banks, public companies, health care
- Quality of information
- Protection of rights
  - Personal data, IPR, etc.
- Regulation of means of security
  - eSignatures, data flows, data storage etc.
- Legal justification in art. 2 of the EU Treaty
  - Sustainable information society development

Business Drivers of Security



Secure application blocks in EU



Other EU Initiatives

- Third Pillar
  - Schengen Information System (SIS)
  - Europol Information System (EIS)
  - Eurodac on fingerprints of asylum seekers and illegal immigrants
  - Biometric passports (ICAO)
  - Confiscation of cybercrime proceeds
  - Cyber terror attacks on computer systems
  - Mutual recognition of confiscation orders

- G5: group on the surveillance of terrorists and criminals on the Internet

EU Standards

- ICT SB / NISSG to follow up EESSI on ETSI SR 002 298:2003
  - http://www.ictsb.org/NISSG_home.htm
- ETSI ESI
- CEN/ISSS eInvoicing WS
- CEN/ISSS 224 -- European Citizen Card
- Need for business registry standards?

Corporate governance

- Proposal for a Directive: amending Council Directives 78/660/EEC and 83/349/EEC concerning the annual accounts of certain types of companies and consolidated accounts – Com(2004) 725 final

- Proposal for a Directive: on statutory audit of annual accounts and consolidated accounts and amending Council Directives 78/660/EEC and 83/349/EEC – COM(2004) 177 final

Some ideas with member state interest

- Clarify the dependencies caused by the legal framework (security/ telco services/ personal data)
- Seek cooperation within the Member State and beyond as appropriate
  - Risk management
  - CERT Cooperation
  - Awareness to SMEs and consumers
- Contribute to the EU standardisation process (98/48/EC) and link to industry standards (ISO 17799, Basel II κλπ.)
  - Physical security and infrastructures (CIP vs. CIIP)
  - Law & Order / Cybercrime (fraud, IPR, child pornography) – 3rd Pillar

Conclusions

- Enhancing the regulatory prospects of information security requires greater involvement at the EU standards level
- End user involvement is needed commensurate with technology penetration
- Exchange of best practices
- Bundling of requirements along application lines:
  - Per sector: eGov, eCom, eBank
  - Per application: eProcurement, eIDM, ePassport, eHealth etc.
  - Per user type: Business, consumer, government etc.

Thank You!

Dr. Andreas Mitrakas
Legal Adviser
ENISA
andreas.mitrakas@enisa.eu.int