# ENISA Workshop on Risk Management

-

Rome – October 2006

**Risk Management in the Banking Sector**

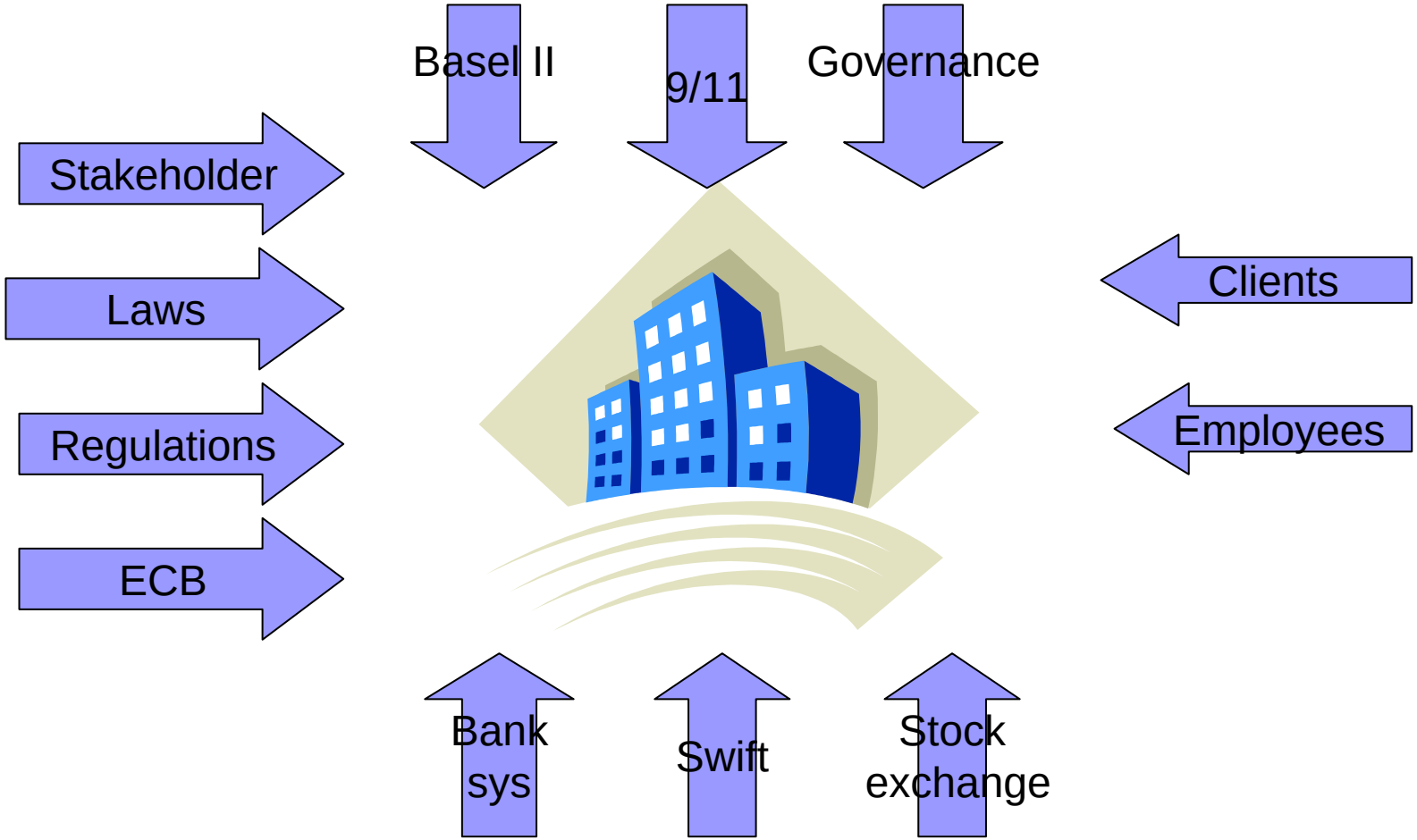
-

**Alain De Greve**

# Introduce myself

- Agronomist (ULB-Brussels)
- Information Technology since 1986 (MF, DBA, Unix, Win, Sec.)
  - Experience in
    - Insurance (500p. Belgium origin, GB subsidiary , IT 30)
    - Telecom ( 1500p. ,GSM , IT 120)
    - Banking ( >35000p , IST >1000)
- Formation - IST related
  - HEC St Louis (Brussels) , MCA (Antwerps) and CISA ( ISACA )
- Contribution to ISO works
  - ISO/IEC/JTC1/SC27 IT Security Techniques (18044,18028,17799,27nnn,…)
  - ISO/TC68 : Banking sector(13569)
- Independent expert for the ENISA (www.enisa.eu.int )
  - Risk assessment / risk management working group
- Collaborate to Clusib (www.clusib.be )
  - Development of “incident management” publication
- Founding member and member of the board of the BCIE (www.bcie.be )

# Banking Sector



# The risks

- What is the importance of information on money for you?
- Who don't have at least one bank account number in Western Europe
  - Issue : East Europe and new potential countries
- Do you still pay with banknotes and coins (without intervention of a bank)?
  - Electronic money
    - Proton in Belgium
    - Internet payments
    - Self bank
- Maximum 10.000 euros for hand by hand transaction
- "supermarket" ATM

# The risk**S** management

# kind of risk ⟺ impact

- Reputation
- Regulatory
- Market
- Liquidity
- Legal
- Business

- Credit
- Systemic
- Compliance
- Strategic
- Merging and acquisition

- People

- …

- Permanence of company
- courts
- Loss in balance sheet
- Payment of clients
- courts
- Parts of market

- Counterparty failure
- 1929 Krach
- jail
- Parts of market , acquisition
- Different technologies and applications

- Social engineering, unwanted awareness, tiger kidnapping…
- …

# The references
# Compliance - constraints

- Operational Risk Management
- Information Risk Management
- Audit
- Cost Accounting
- Human Resources, Legal…
- Others
- Governance
- Basel II
- ISO 2700x series and 25700
- Cobit 4
- IFRS , IAS
- Law on Privacy, local laws
- Laws and regulations in general
- European directives
- Local codes (Lippens, Tabaksblat,…

# Information technology operating systems - applications

- Banks have different platform solutions
  - Mainframe, midrange, distributed
- Each have their own risks
  - Mainframe – old applications- knowledge of engineers and programmers
  - Midrange – different OS specificities ( Unix's, i5, Linux,…)
  - Distributed : Windows…. Open Office
  - …old stuff
- Value and quality of transactions
  - Confidentiality, Integrity, Availability ……Non repudiation
  - Money Laundering
  - International Payments ( SWIFT system)
  - Reputation ( scandal , not tiger kidnapping but error on placement or network connectivity – timestamp for transactions))
  - Web applications
  - Security of file transfer
  - Encryption

# Networking aspect

- Communications between banks
  - Chamber of compensation , CEC,…
- Stock Exchange
  - Just in time
- Swift
  - Big amounts
- Clients
    - Home banking
    - Web-banking
    - ATM
    - Credit request and control

# Some specific sector risks (IST related)

- Phishing
  - Bank accounts capture, password retrieval
    - Solution : complex identification methods
- Spam
  - General email-address, decrease productivity of employees
- Canada dry
  - It looks like an official site but… is not a bank site
- Web site defacement
- Cryptography and non-repudiation

# Future needs

- Growing size of Europe
- Position of the Euro
- Standardization view
  - Initiative of the ISO regarding risk management in 27005 and 25700
- Interoperability debit and credit cards
- Need to develop
  - Standard
  - Method
  - Processes
  - Procedures

# Future requirements

- Compliance to all local laws and regulations (+ EU laws)
- Incorporation of Turkey, Romania, Bulgaria, etc.)
- USA (or other) wishes
- Stock Exchange
- Impact of outsourcing or co-sourcing
- Where are the financial and privacy data's?
- Integration  with e-id , different cards and chips
- Dematerialization of money
- Money without frontiers

# Future solutions

- Contact with external organization and supporting initiatives to be sure to remain aligned with sector specificities
- Cooperation between bank as well on local level than on European level (ECBS)
- Implement solution and good practice like those in ISO/IEC IS 17799:2005 (27002)
- Interoperability, common language
- Biometrics, cryptography
- Specific Bank sector ISO standards ( ISO/TC68 , ISO/IEC/JTC1/SC27 , …)

# Relevant web sites

- Basel II http://www.bis.org/publ/bcbsca03.pdf
- Sox http://www.legalarchiver.org/soa.htm

- ISO/IEC/JTC1/JSC27 : www.din.de/sc27
- ISO/TC68 : www.iso.org/tc68.
- ENISA www.enisa.eu.int/rmra ...

- Code Lippens (Belgian corporate governance (9 December 2004 )) http://www.corporategovernancecommittee.be/library/documents/final%20code/CorpGov_FR5.pdf
- Luxemburg (CSSF): http://www.cssf.lu/index.php?id=22
- France : http://www.amf-france.org/documents/general/6896_1.pdf
- Netherlands : Tabaksblat (9 December 2003 )
- ECB : www.ecb.int

# *Thank You for your attention*


# *Q & A*

*For further information* .**E-mail : alain.degreve@skynet.be**