



# Information Security Regulation: Compliance and Non-Compliance

Dr. Tommy Tranvik, NRCCL,  
University of Oslo

# The Research Project



- Compliance: the implementation and use of information security regulations
- Top-down: the Data Inspectorate (and other national actors)
- Bottom-up: municipalities and municipal ICT companies
- 26 municipalities
- 17 % of the population

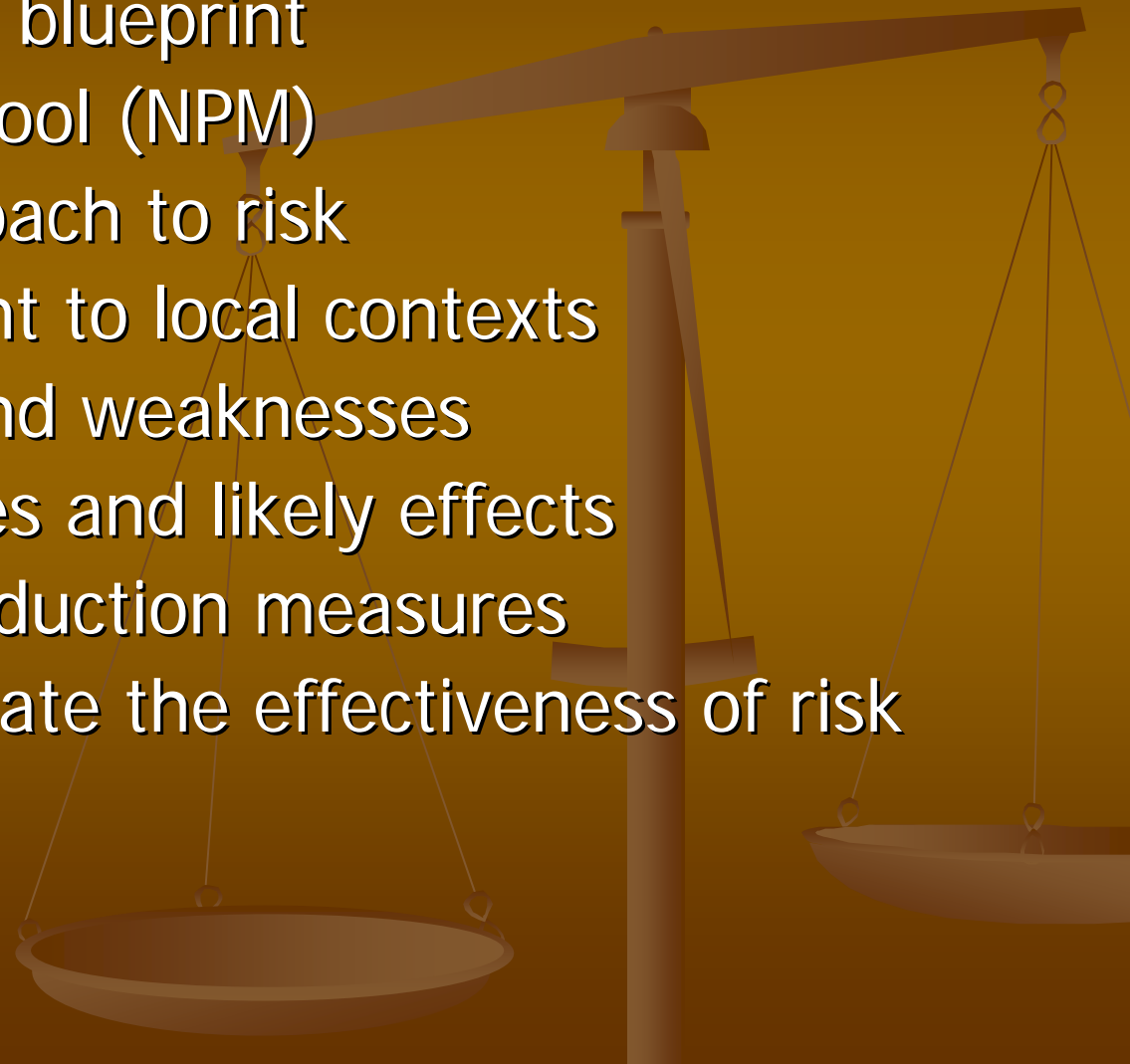
# Legal Requirements



- Section 13 (DPA), chapter 2 (DPR)
- Positive rather than negative action
- Enhance data protection and privacy rights
- Implement "planned and systematic measures"
- Provide "a sufficient level of information security"
- Define risk criteria: what is "sufficient"?
- Decide on the risk reducing measures

# IS and Risk Management

- Risk management blueprint
- Decision-making tool (NPM)
- Engineering approach to risk
- Adapt the blueprint to local contexts
- Identify threats and weaknesses
- Assess probabilities and likely effects
- Implement risk reduction measures
- Monitor and evaluate the effectiveness of risk reduction

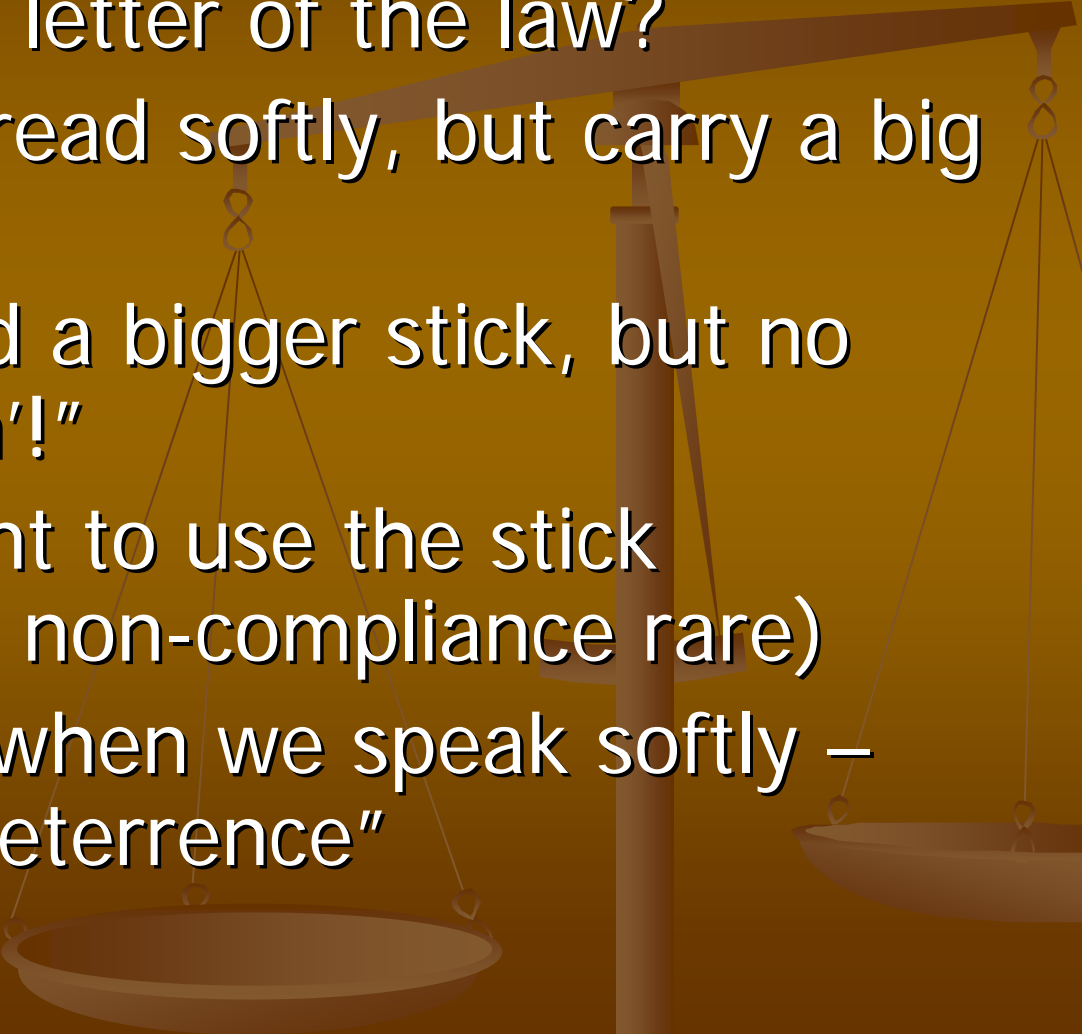


# Regulatory Approach

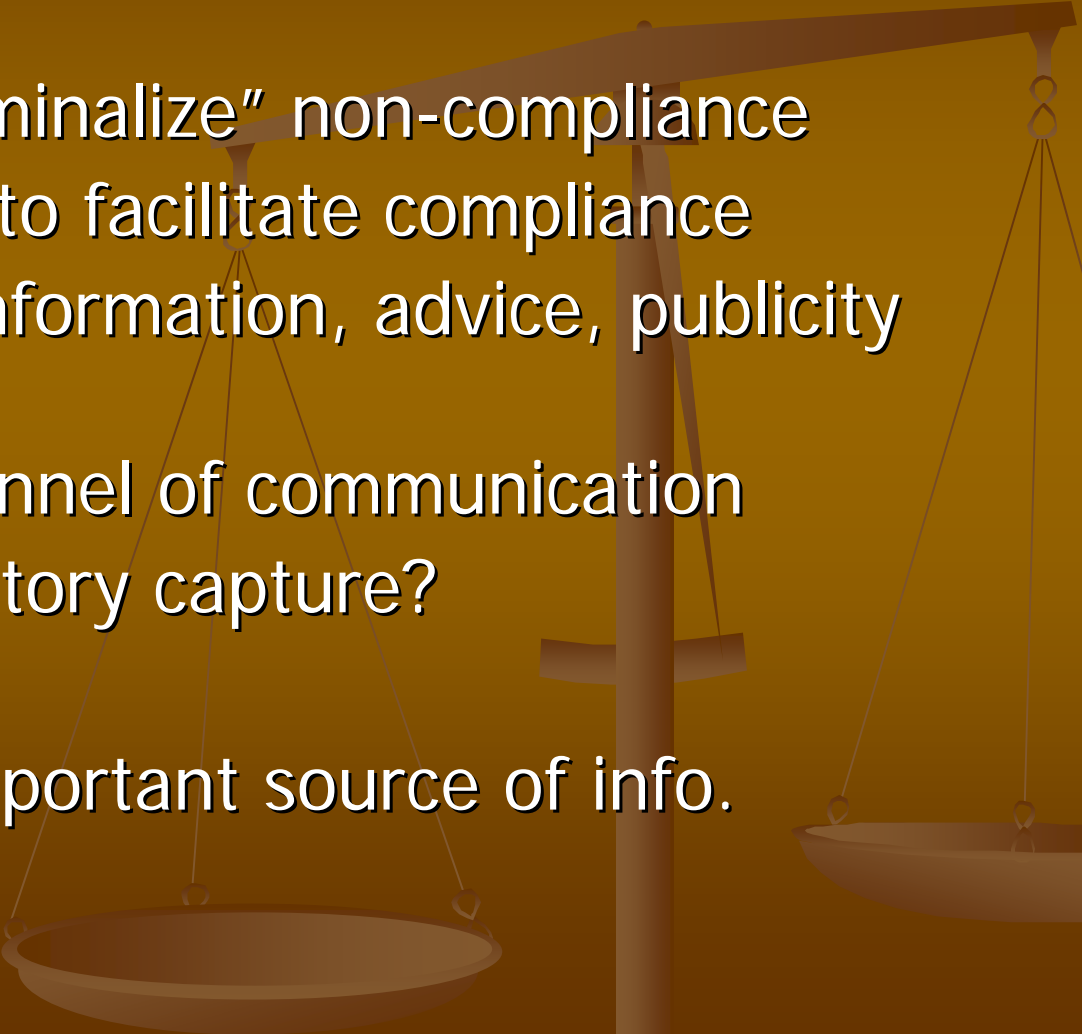


- Enforced self-regulation = state regulation + legalization
- State regulation: the enforcement of state rules by public agencies
- Inspections and sanctions
- Legalization: domestication of legal requirements (risk management)
- The adaptation of the risk management blueprint – internalize regulatory goals

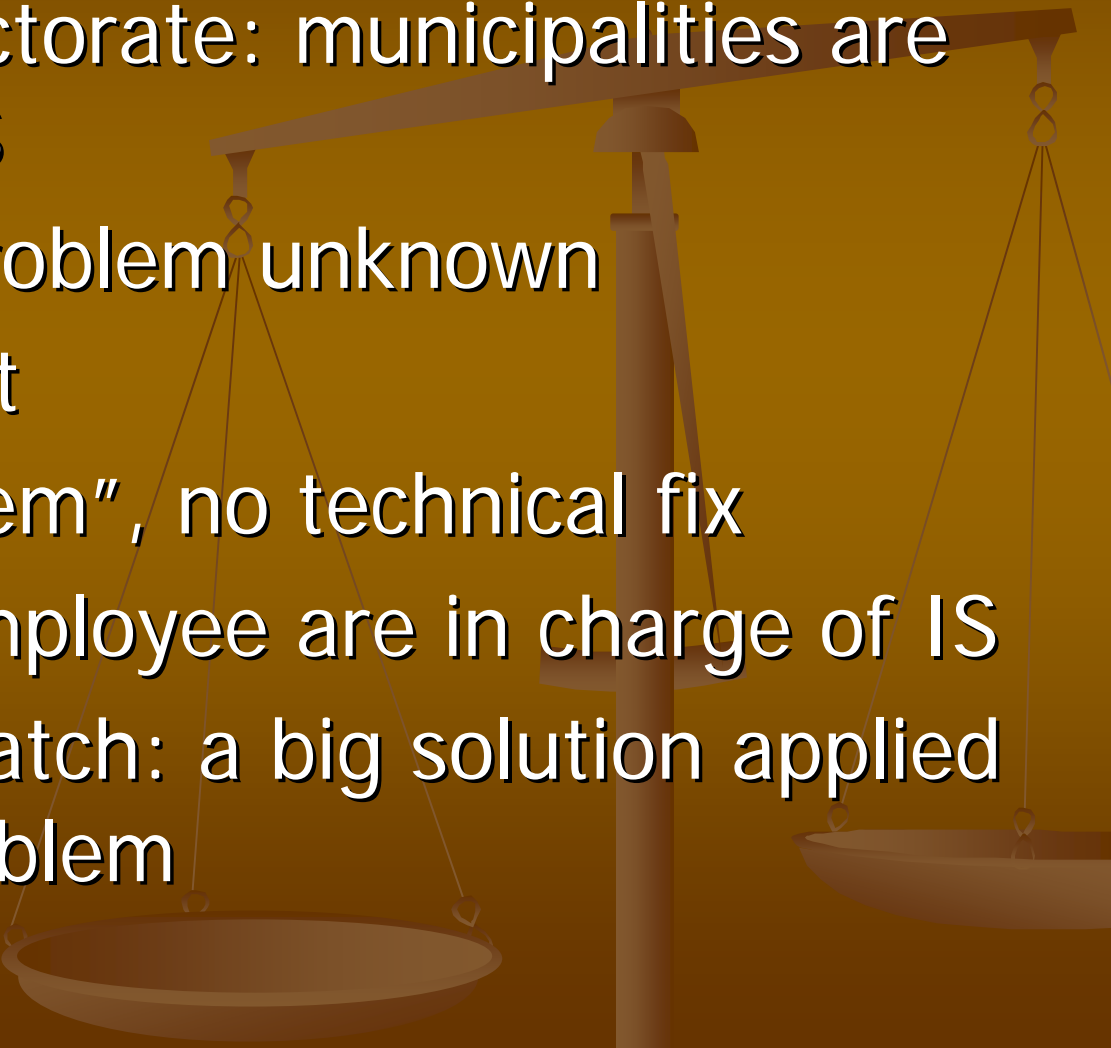
# Regulation and The Data Inspectorate

- The spirit or the letter of the law?
  - Philosophy: "Thread softly, but carry a big stick"
  - Claim: "We need a bigger stick, but no 'nuclear weapon'!"
  - Reality: Reluctant to use the stick (punishment for non-compliance rare)
  - "More effective when we speak softly – the stick is for deterrence"
- 

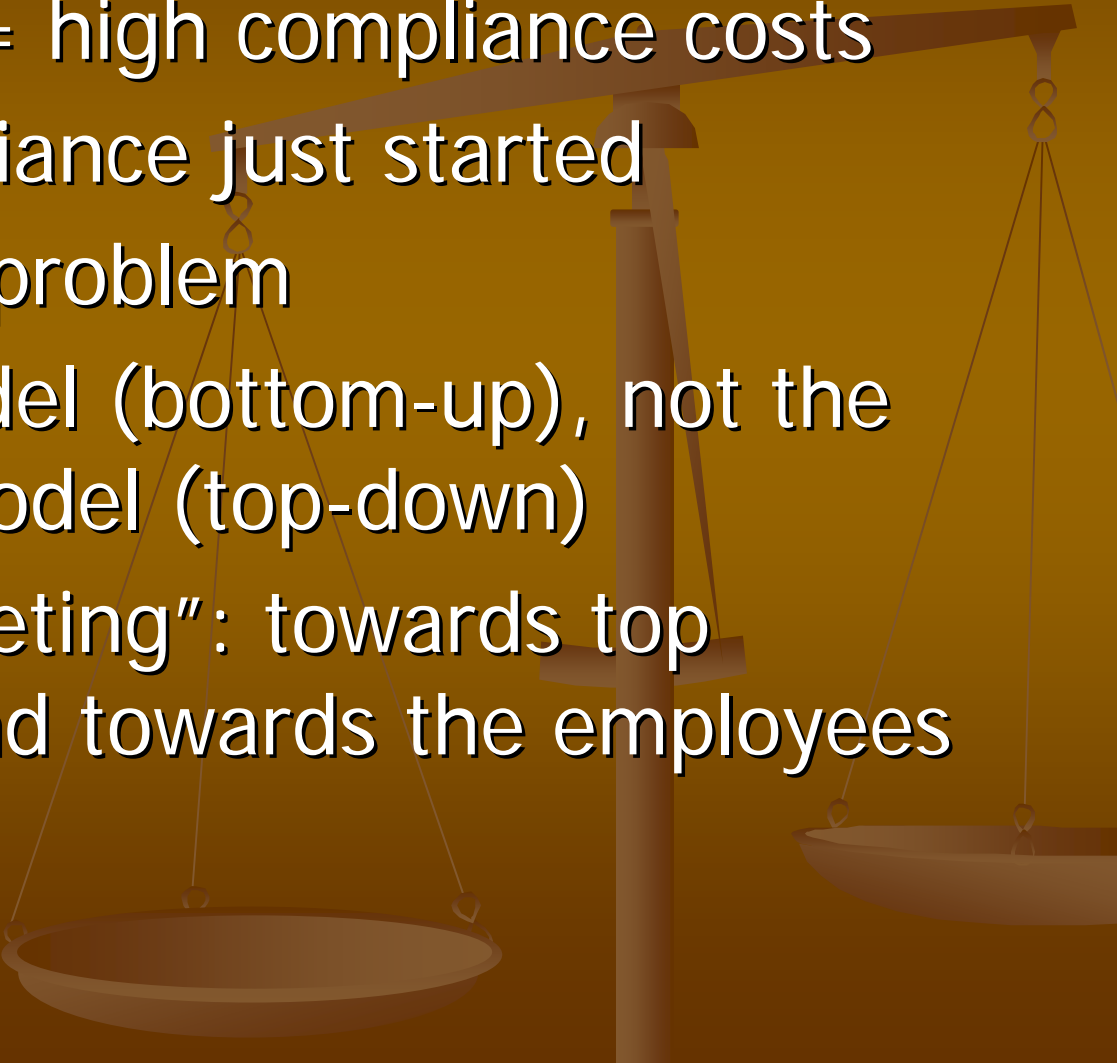
# Regulation and The Data Inspectorate

- Don't want to "criminalize" non-compliance
  - Need cooperation to facilitate compliance
  - Important tools: information, advice, publicity (shaming)
  - Inspections: a channel of communication
  - Evidence of regulatory capture?
  - Regulatory deficit
  - Municipal view: important source of info.
- 

# Information Security and Municipalities

- The Data Inspectorate: municipalities are serious about IS
  - Size of the IS problem unknown
  - Probably modest
  - A “people problem”, no technical fix
  - Even so: ICT-employee are in charge of IS
  - Perceived mismatch: a big solution applied to a modest problem
- 

# Legalization and Municipalities

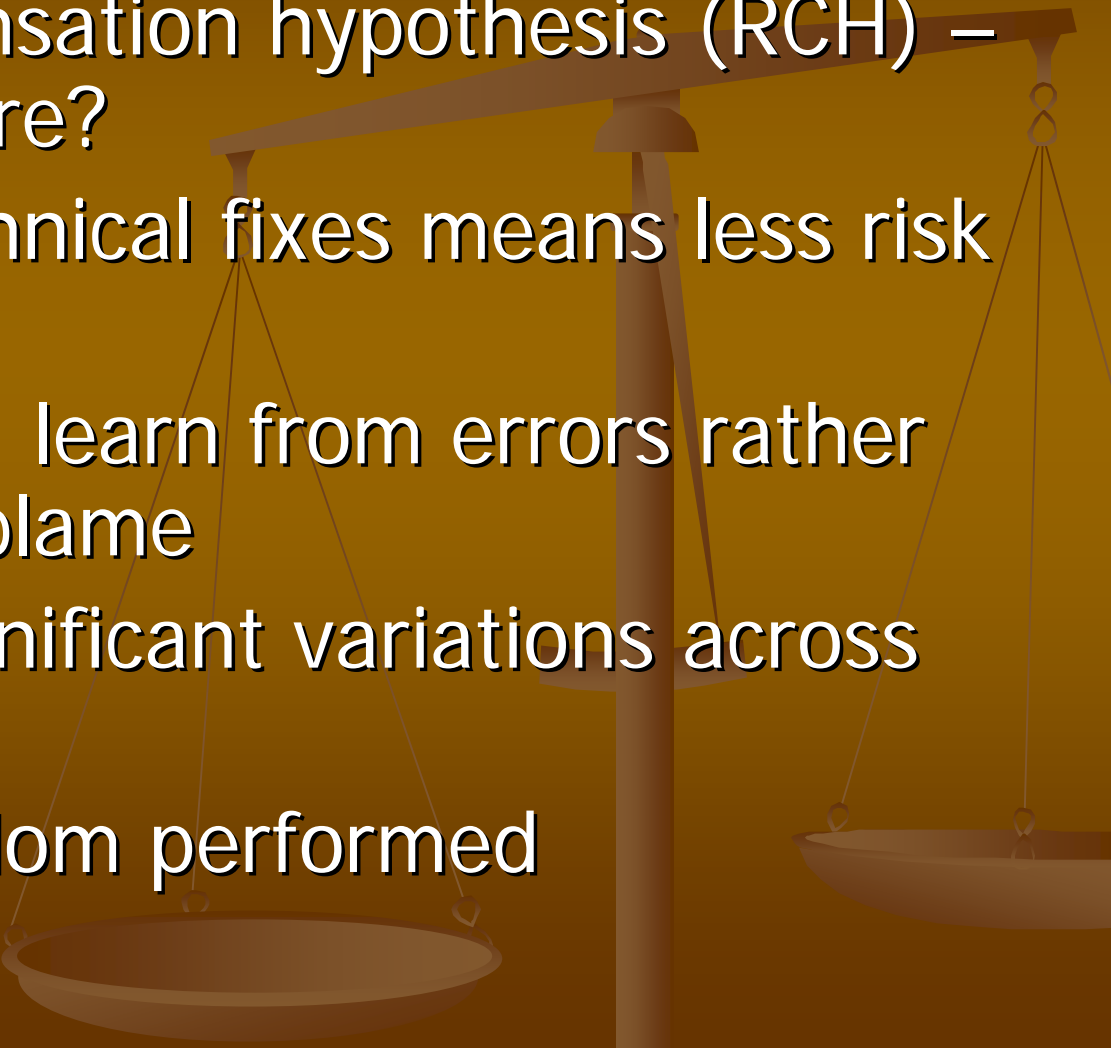
- Positive action = high compliance costs
  - Municipal compliance just started
  - The translation problem
  - The idealist model (bottom-up), not the management model (top-down)
  - Two-way “marketing”: towards top management and towards the employees
- 

# Legalization and Municipalities

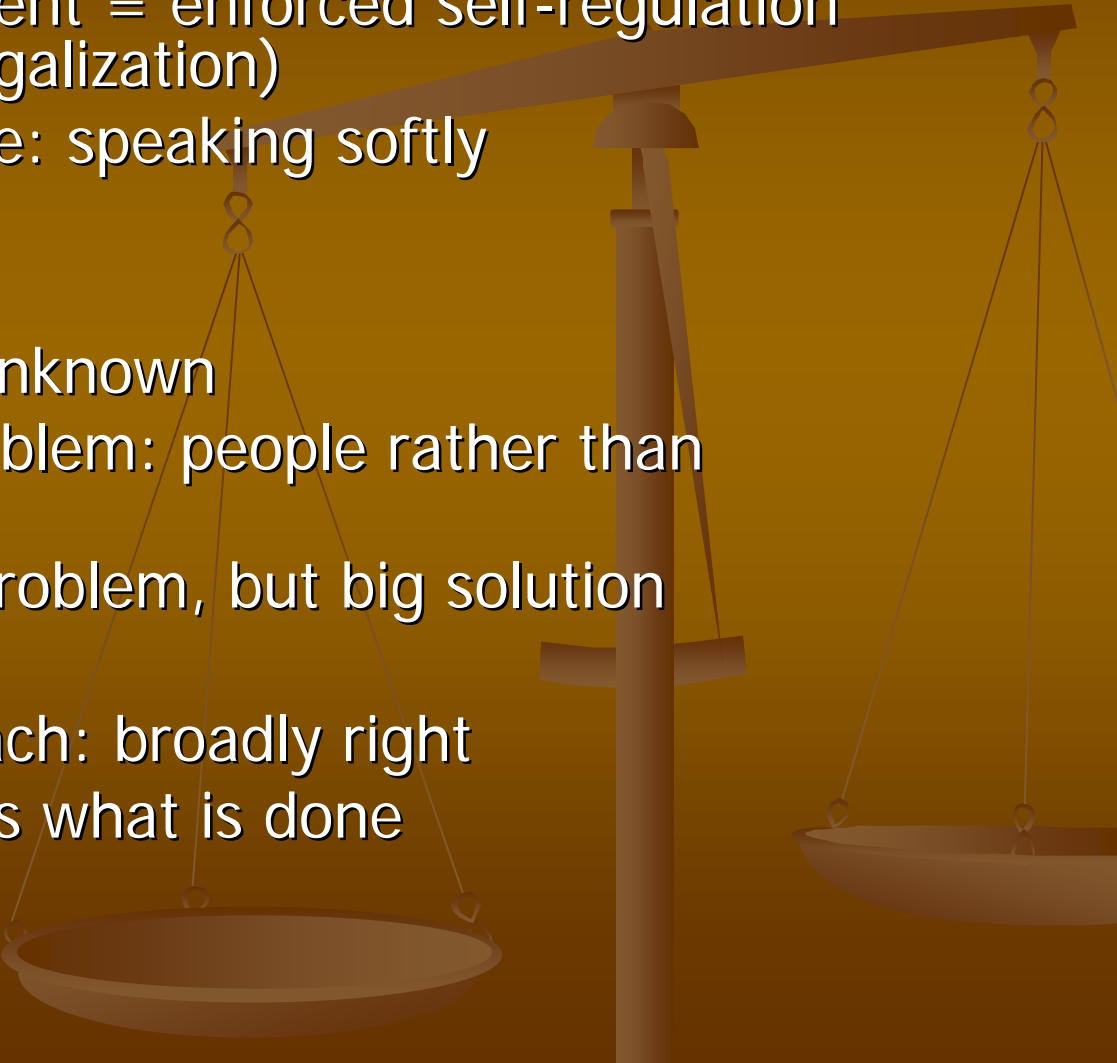


- The IS risk management system exist on paper
- Usually not practiced as advertised
- “We get the money to buy new technology, but not the attention to deal with the people problem”
- Risk assessment approach: “broadly right rather than precisely wrong”
- RA applied on a random basis
- RA expertise: learning by doing
- Focus no data protection and privacy?

# Legalization and Municipalities

- The risk compensation hypothesis (RCH) – does it apply here?
  - RCH: better technical fixes means less risk awareness?
  - Risk monitoring: learn from errors rather than distribute blame
  - Risk culture: significant variations across professions
  - Risk audits: seldom performed
- 

# Empirical conclusions

- IS and risk management = enforced self-regulation (state regulation + legalization)
  - The Data Inspectorate: speaking softly
  - spirit over letter?
  - Regulatory deficit
  - Size of the problem unknown
  - The nature of the problem: people rather than technology
  - Perception: modest problem, but big solution
  - The idealist model
  - Qualitative RA approach: broadly right
  - What is written versus what is done
- 

# Normative conclusions

- Machines are built to comply: they follow authoritative rules and are easily programmable
  - People are not built to comply: they do not always follow authoritative rules and may not be easily programmable
  - Compliance is therefore a messy process – the outcome may be unpredictable
  - Cannot regulate people on the assumption that they behave like machines
  - Is risk management “the mother of all solutions”?
- 