

# Information Security in Social Media

Challenges for Corporate IT strategy

**Dr. Lothar Fritsch**  
**Norsk Regnesentral**

«Inclusive Identity Management in Social Media»

**e-Me** Seminar, Oslo, 22. March 2011

# Dr. Lothar Fritsch

- ▶ Research Scientist in IT Security & Privacy in Norsk Regnesentral's ICT research department
- ▶ Master from University of Saarland
- ▶ Graduate studies and PhD at Frankfurt's Goethe University's Information Systems department
- ▶ Industry experience in IT security product management
- ▶ Participant in EU PET research, e.g. SEMPER, PRIME, FIDIS and national projects

Web: [www.nr.no/~lothar](http://www.nr.no/~lothar)



**NR** Norsk Regnesentral  
NORWEGIAN COMPUTING CENTER

**Lothar Fritsch**

forsker · research scientist  
DART · department of applied  
research in information technology

dir. phone: (+47) 22 85 26 03  
mob. phone: (+47) 968 85 758  
[Lothar.Fritsch@nr.no](mailto:Lothar.Fritsch@nr.no)

Norsk Regnesentral · Norwegian Computing Center  
Gautstadalleen 23, P.O. Box 114, Blindern  
NO-0314 Oslo, Norway  
[www.nr.no](http://www.nr.no) · [nr@nr.no](mailto:nr@nr.no)

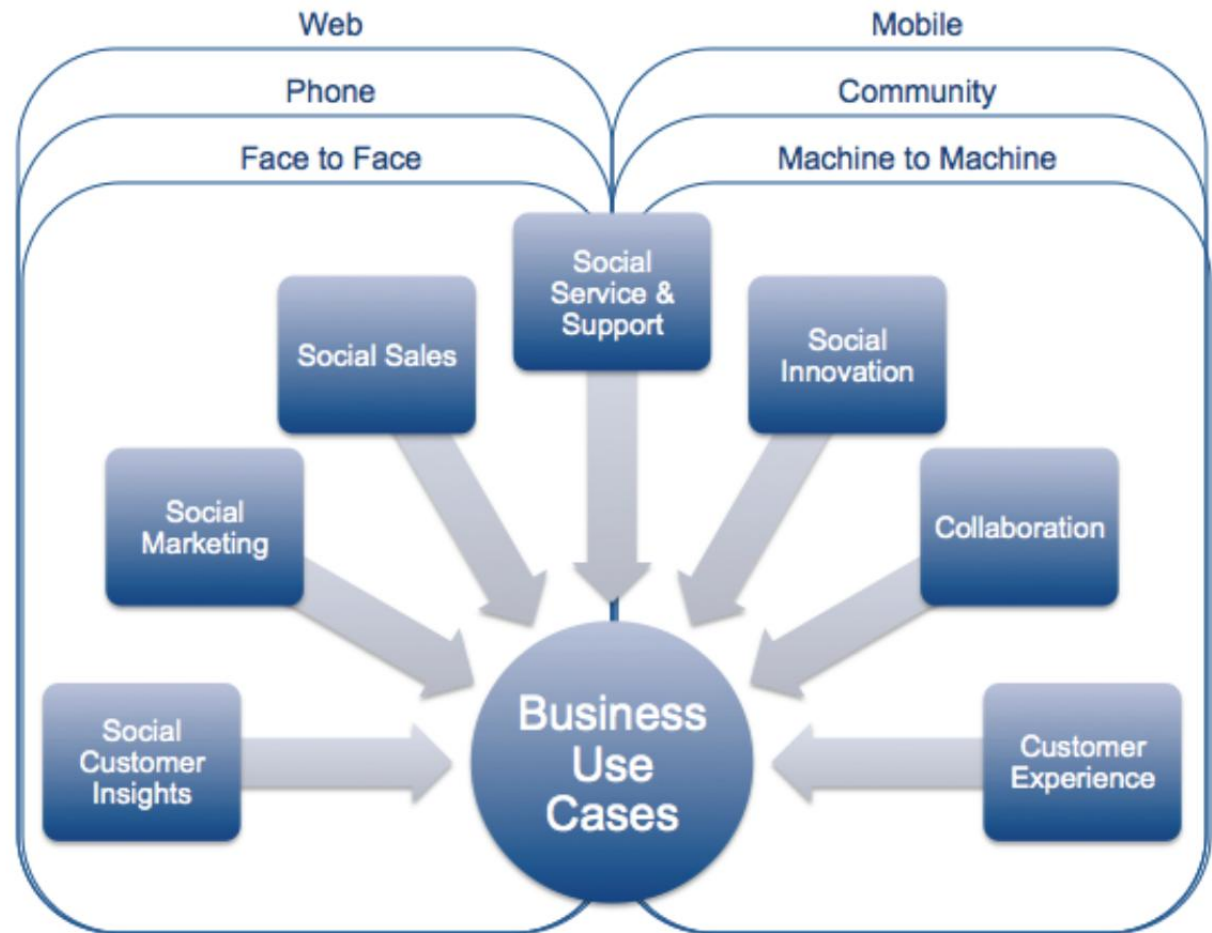
phone: (+47) 22 85 25 00  
fax: (+47) 22 69 76 60

# Agenda

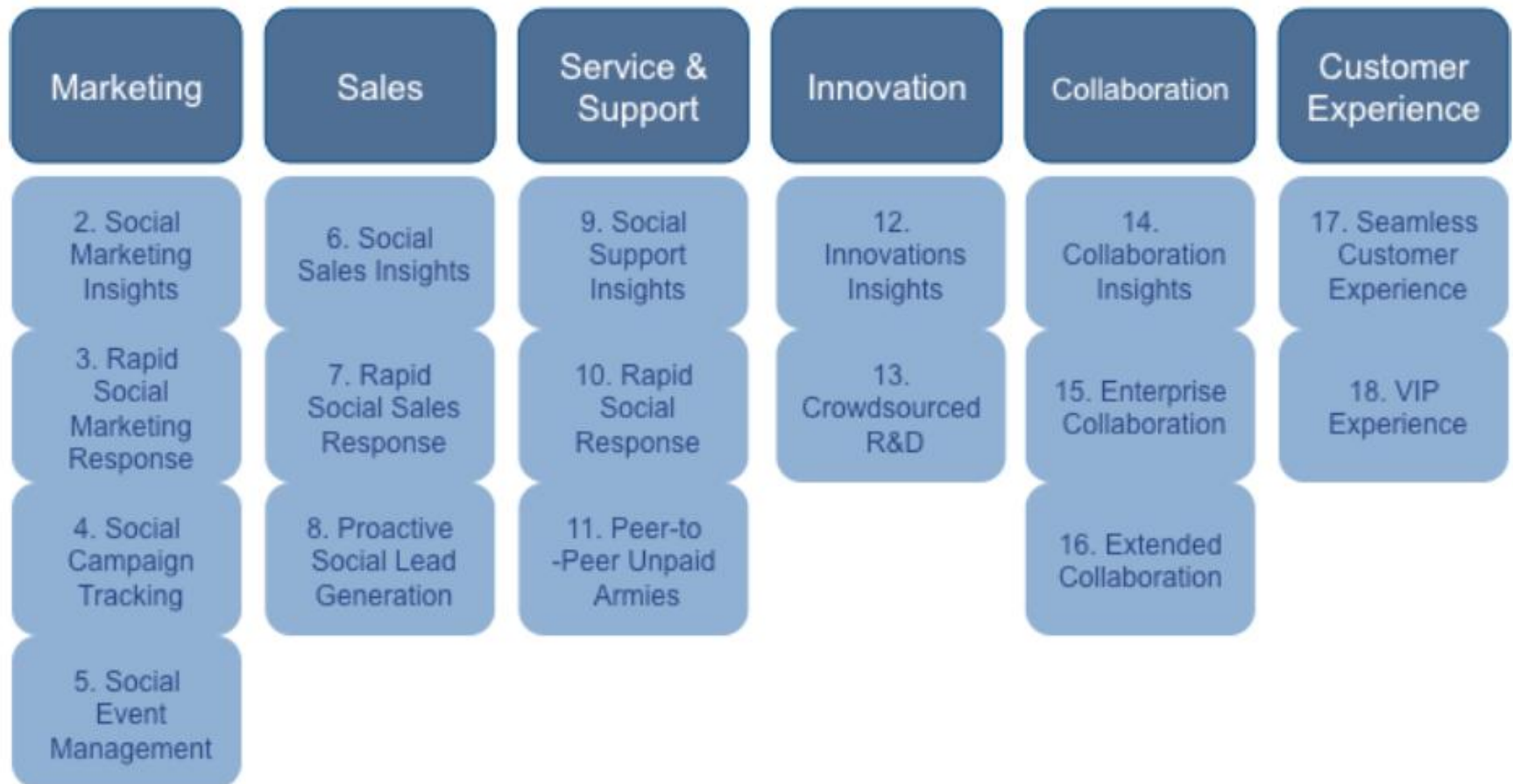
- ▶ Corporate use of Social Media
- ▶ Organization and Responsibilities
  - IT operations
  - Roles
  - Regulatory compliance
- ▶ Challenges and Technological Approaches
  - E-ID and Identity Management
  - Authorization and Internal Processes
  - Ownership and Copyright Issues

# Use: New communication channel

- ▶ Social Media are an additional channel for corporate communication.
- ▶ Communication processes and roles are often organized for older channels. But new channels might create temporary confusion.



# Use: Purpose of Social Media

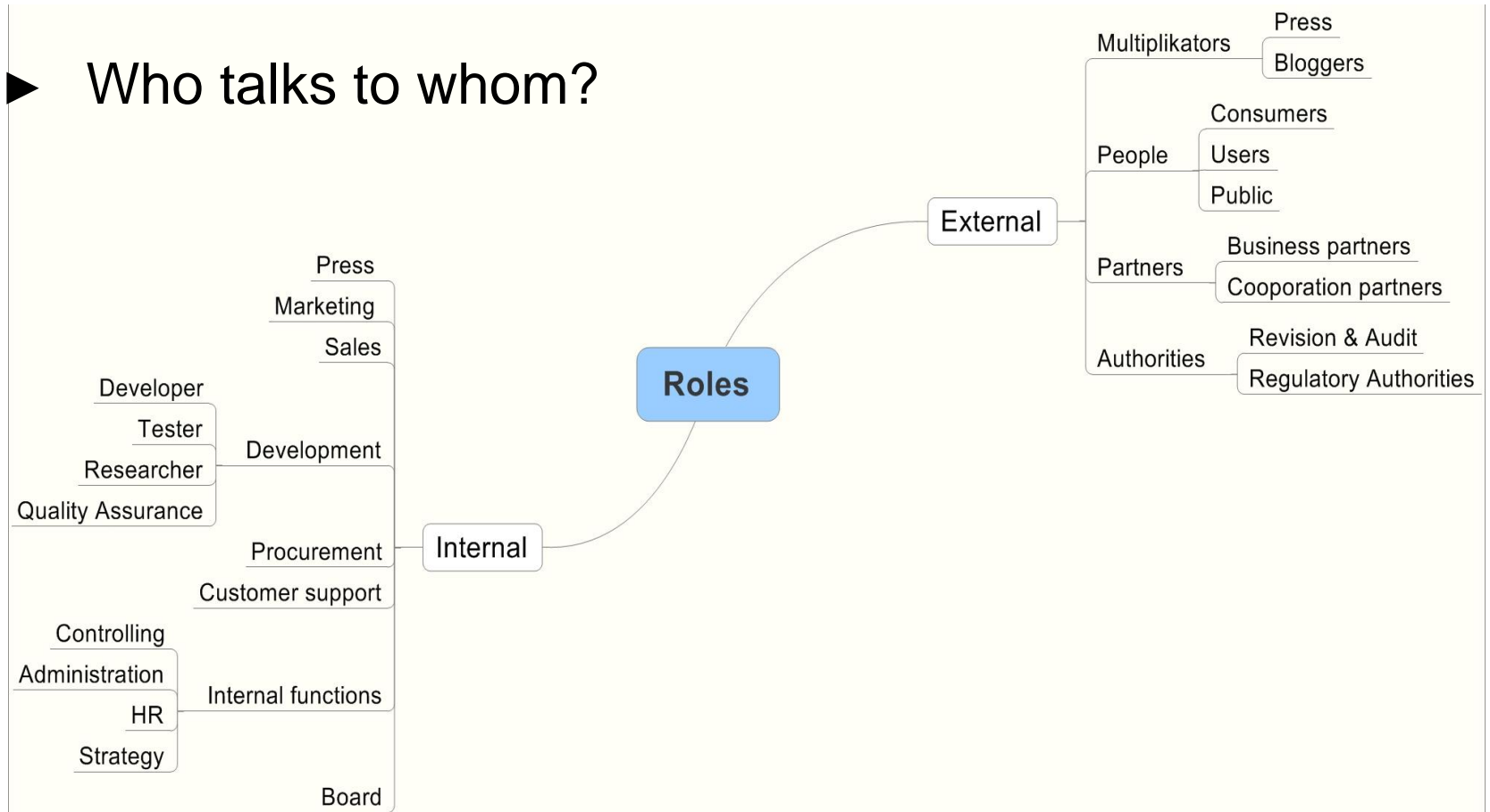


# Organization and Responsibilities

- ▶ Who owns data, processes, governance and responsibility?
  - Own organization? IT department? Risk panel? Board? Facebook?
- ▶ Who controls 'e-ID's and profiles?
  - Platform vendor, platform owner, own organization, users, 3rd party provider?
- ▶ Are there any contracts on service levels?
  - Reaction time, Ownership, SPAM, DDOS, defacing, data breach, access to data, compliance?

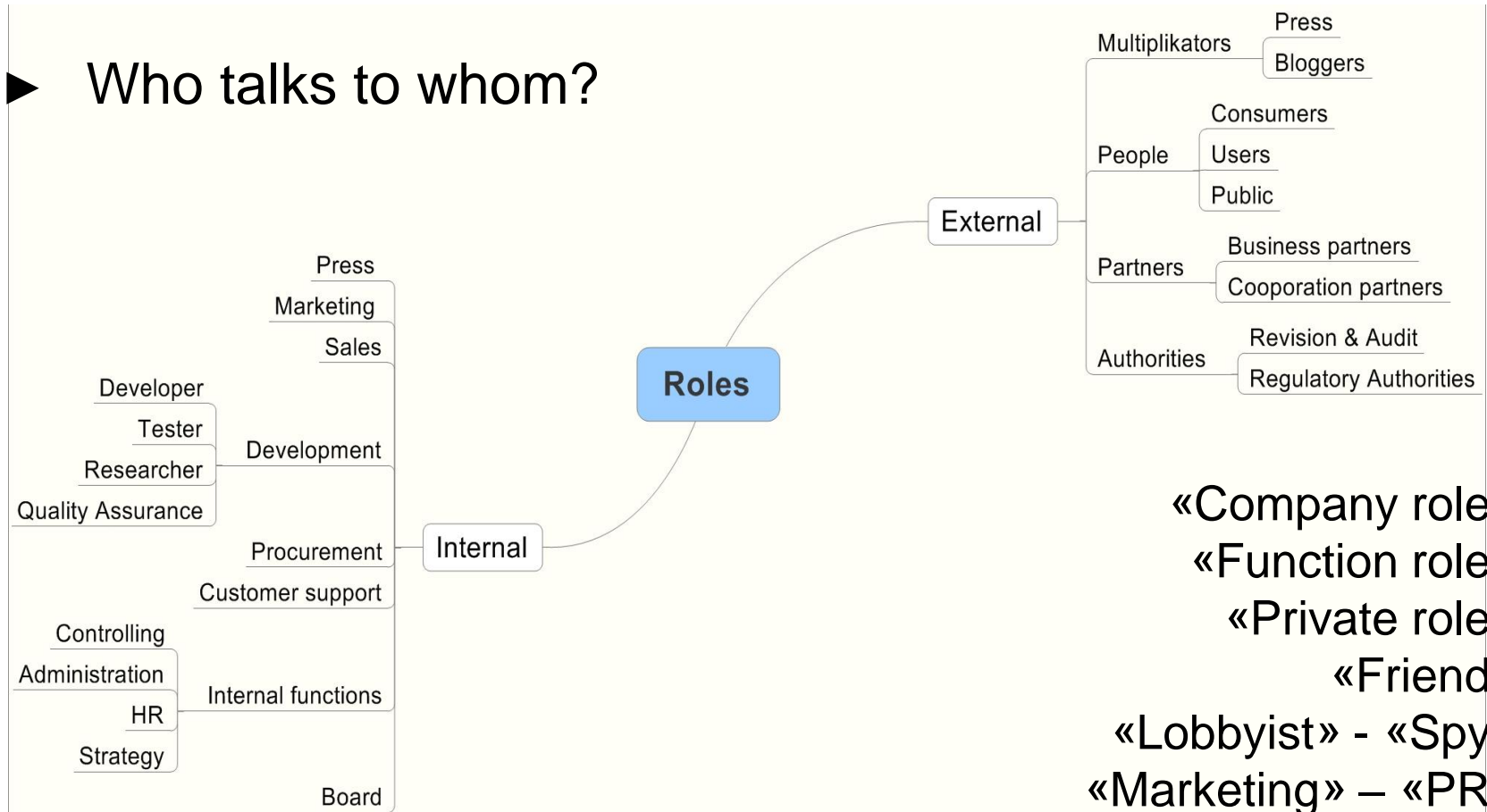
# Corporate roles in Social Media

## Who talks to whom?



# Corporate roles in Social Media

## Who talks to whom?



It is necessary to keep roles separate!

# Regulatory limits of Social Media

## Examples:

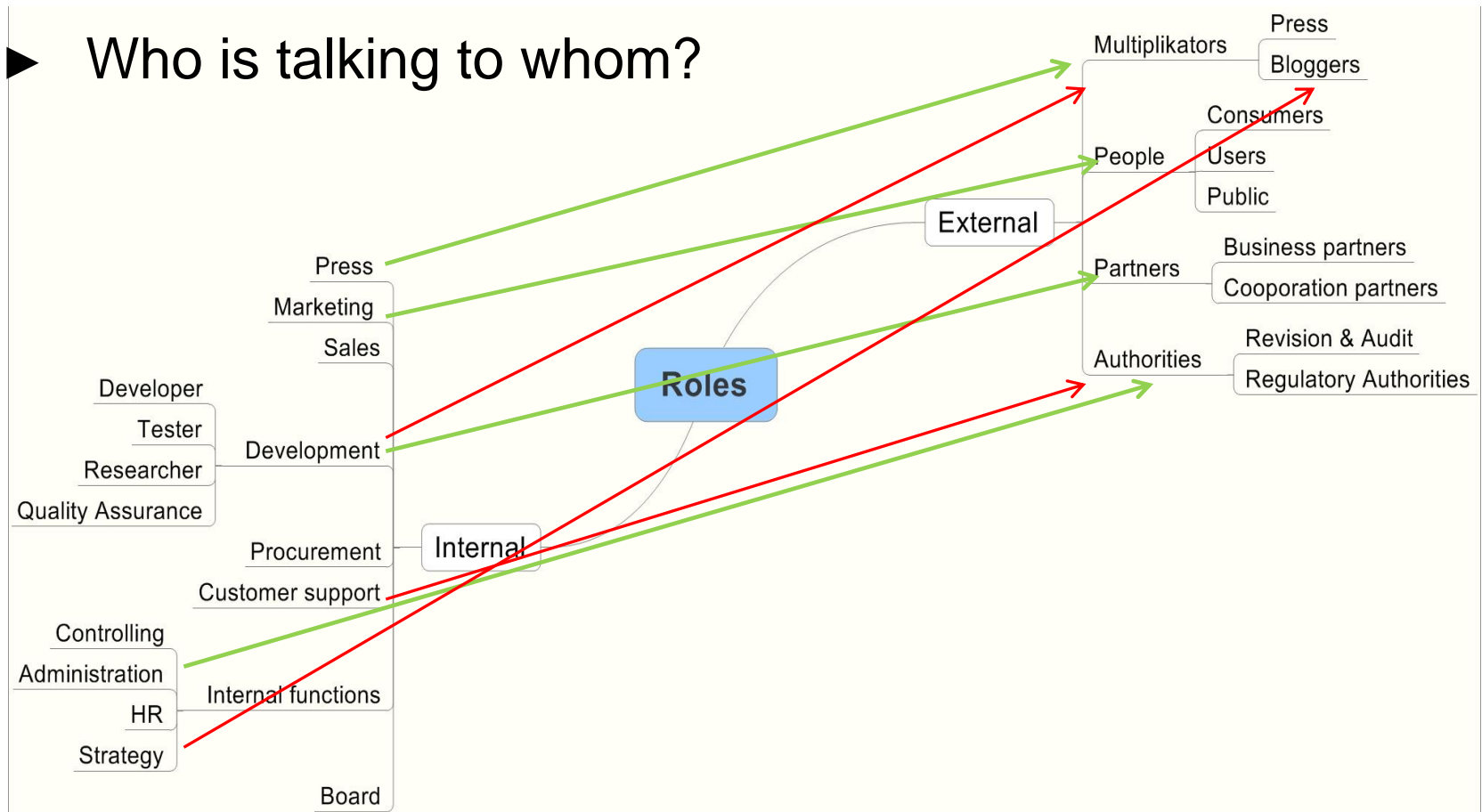
- ▶ Age verification (legal age?)
- ▶ Privacy and data protection, consent, information rights
- ▶ Responsibility for wrongful personal data, loss or its abuse.
- ▶ Business secrets and classified documents
- ▶ Health sector regulation
- ▶ Financial market requirements
- ▶ Civil liability with public advising in Social Media

# Challenge: Identity Management

- ▶ Authenticity of persons and e-ID
  - Who is talking on behalf of the organization? In which role?
  - Who are we actually talking to?
  - Who does that person have access to within our groups/staff/information?
  - Who owns and manages these e-IDs?
- ▶ ID theft can expose internal affairs to other parties.
- ▶ Risk analysis for both the organization's immaterial assets (customers, innovation, reputation) and for IDM and security concepts on the Social Medium.

# Communication Roles in Social Media

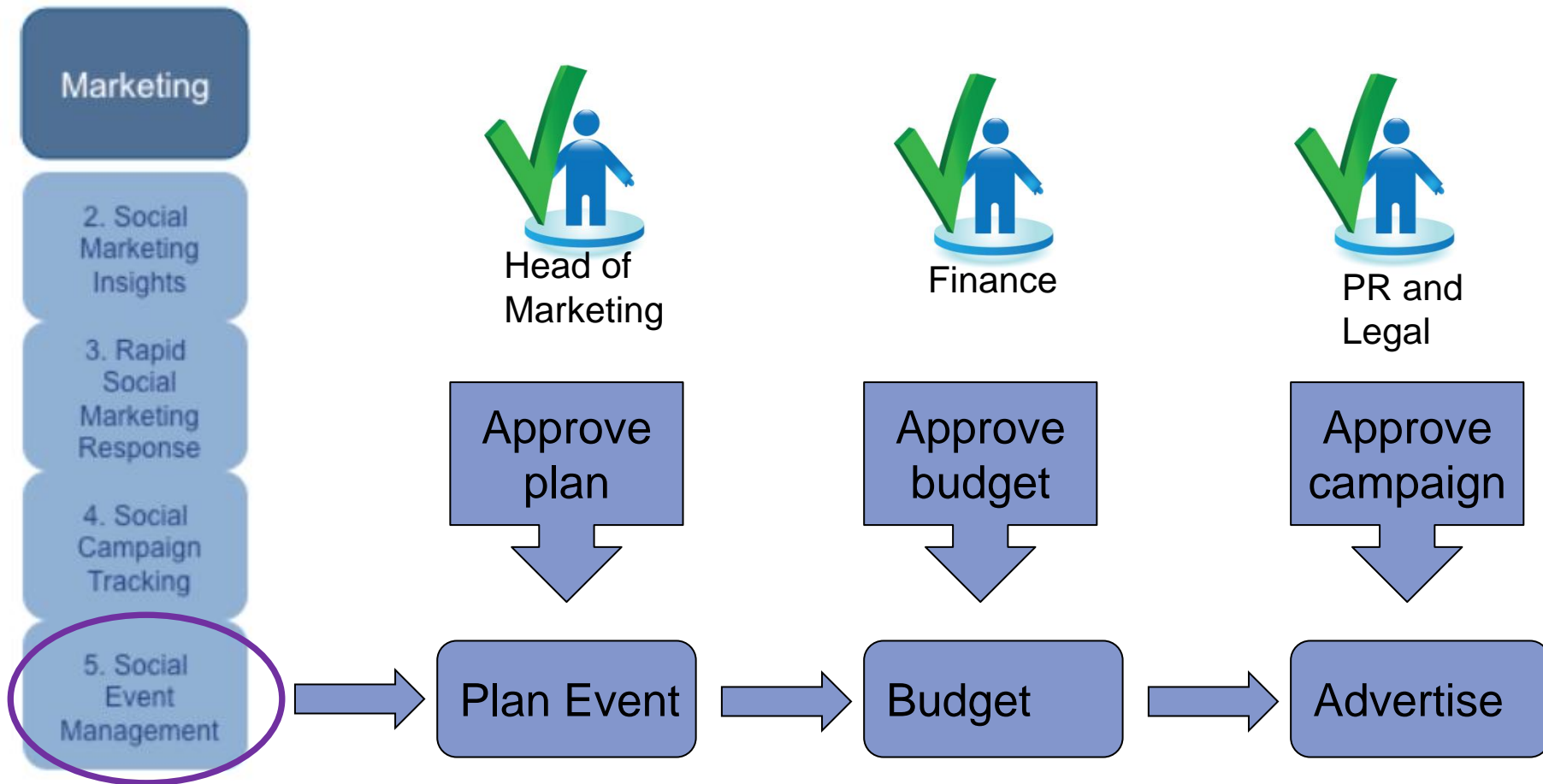
## Who is talking to whom?



# Challenge: Authorization & Responsibility

- ▶ Many processes need authorization from a person with a certain role, or certain privileges.
- ▶ Press officers or the legal department often clear public statements on behalf of a company.
  - There is a significant difference between a company's official statements and its employees' personal statements.
  - Stock exchange listed corporations might have report duties that get undermined by employees public tale.
- ▶ Both a policy for use of Social Media and well-defined roles for various functions are useful.
- ▶ Processes with explicit authorization, esp. concerning confidential documents or regulated issues, are needed.

# Authorization process example



Where is the border between management information system, social media, and corporate archive? Who controls them?

# Challenge: Integrity & Ownership

- ▶ Falsification vs. authenticity of content
  - integrity on archives, authentic e-identities and roles, non-repudiation
- ▶ Copyright (Crowdsourcing) and origin
  - Participants in innovation processes should comply to policy/NDA – and conform to a security policy!
- ▶ Physical and virtual control (Access, Backup, Deletion)
  - Who owns disk, database and content?
- ▶ Access control and usage policies for users
- ▶ Mechanisms for information flow control

# Content, Origin, and Ownership

Innovation

12.  
Innovations  
Insights



Origin and copyright of ideas? Plagiarism?

13.  
Crowdsourced  
R&D



Is there an agreement? Confidentiality? Roles defined?  
Ownership issues?

# Summary

- ▶ Separate professional and private roles on Social Media
  - Use different profiles for different roles
  - Don't blend networks that belong to different roles!
- ▶ Create awareness of secrecy requirements, sensitive data, and business secrets
  - Restrictive content management, explicit policy
  - Block access to Social Media in critical offices
  - Clearly defined responsibilities and authorization processes
- ▶ Protect business interests against platform owner and other users
  - Copyright, ownership issues (hardware, access, database)
  - Registration, administration of users (Identity Management)

**If social tools don't cost you anything,  
then it's you who is  
being sold for someone else's profit.**