



**Institutional context of the adoption
of ISO/IEC 27001/27002 in China**

Xu Yang, Henk J. de Vries

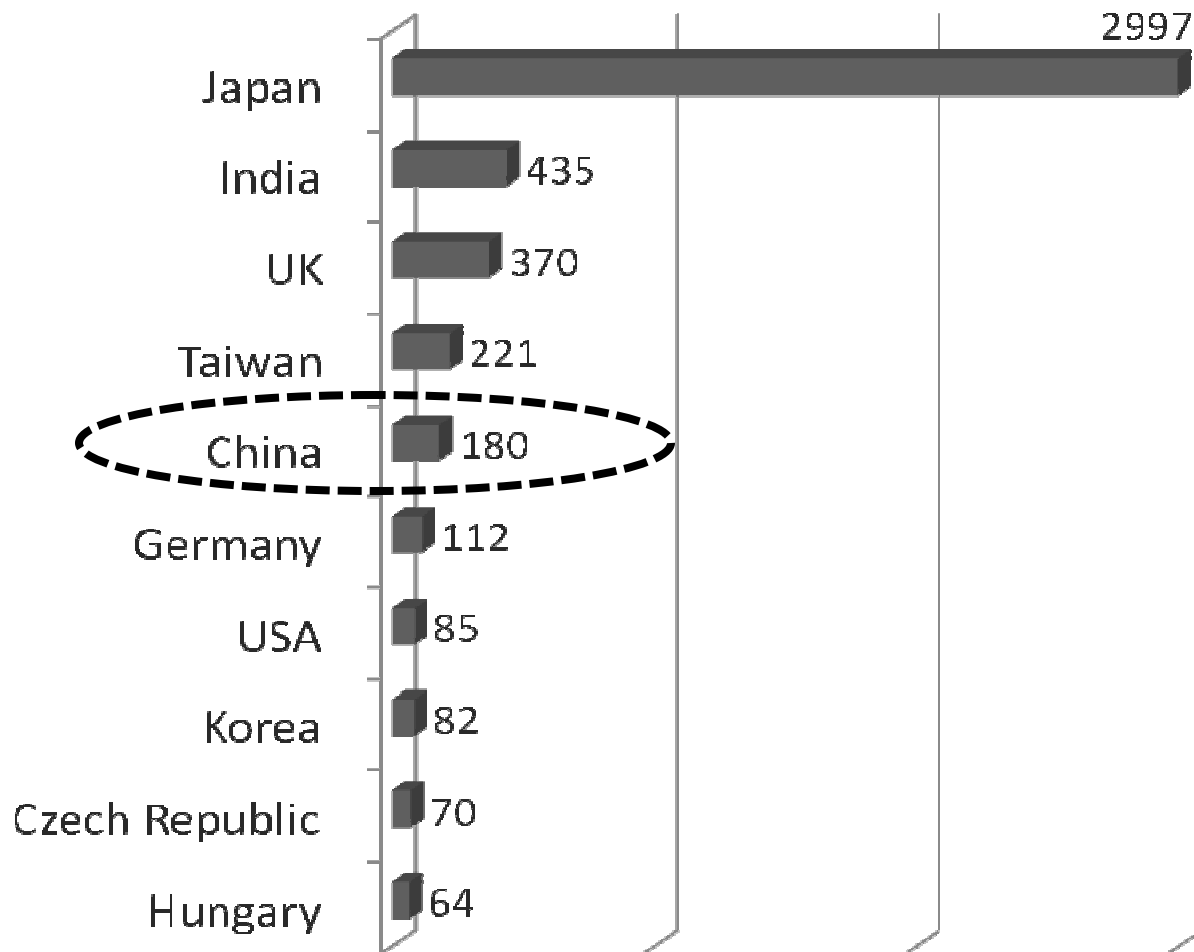
Institutional context of the adoption of ISO/IEC 27001/27002 in China

- Introduction
- Research approach
- Potential stakeholders
- Parties involved in the transformation of ISO/IEC 27001/27002
- Parties involved in the implementation of ISO/IEC 27001/27002
- Discussion & Conclusions

[Introduction]

- The adoption of ISO/IEC 27001/27002
 - ISO/IEC 27001:2005 → GB/T 22080-2008
 - ISO/IEC 27002:2005 → GB/T 22081-2008
- “GB/T”: National/Recommendatory standards
- “IDT”: Identical adoption

ISO/IEC 27001 certificates of China



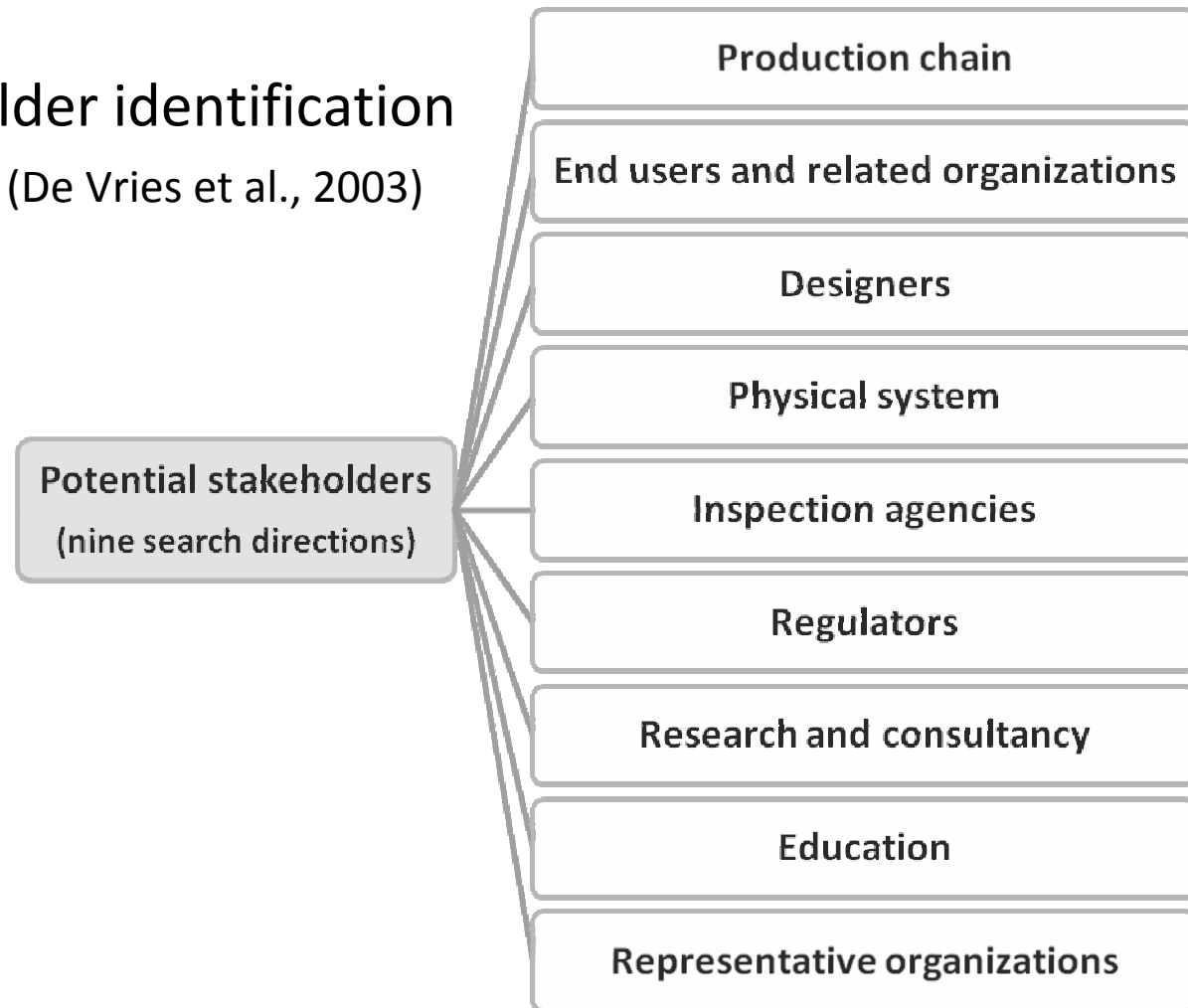
Source: ISMS International User Group (IUG), 2009.1, Version 188.

[Research topic]

- Potential stakeholders related to ISO/IEC 27001/27002 adoption in China
- Parties involved in the adoption of these standards as Chinese standards
- Organizations which implemented these standards
- Discussion and conclusions

Research approach

- Stakeholder identification method (De Vries et al., 2003)



Parties involved in the transformation of ISO/IEC 27001/27002

- **Governor & Technical Committee**
 - SAC: Standardization Administration of the People's Republic of China - Regulators
 - TC260: China Information Security Standardization Technical Committee - Regulators
- **Proposer**
 - MIIT: Ministry of Industry and Information Technology of the People's Republic of China - Regulators

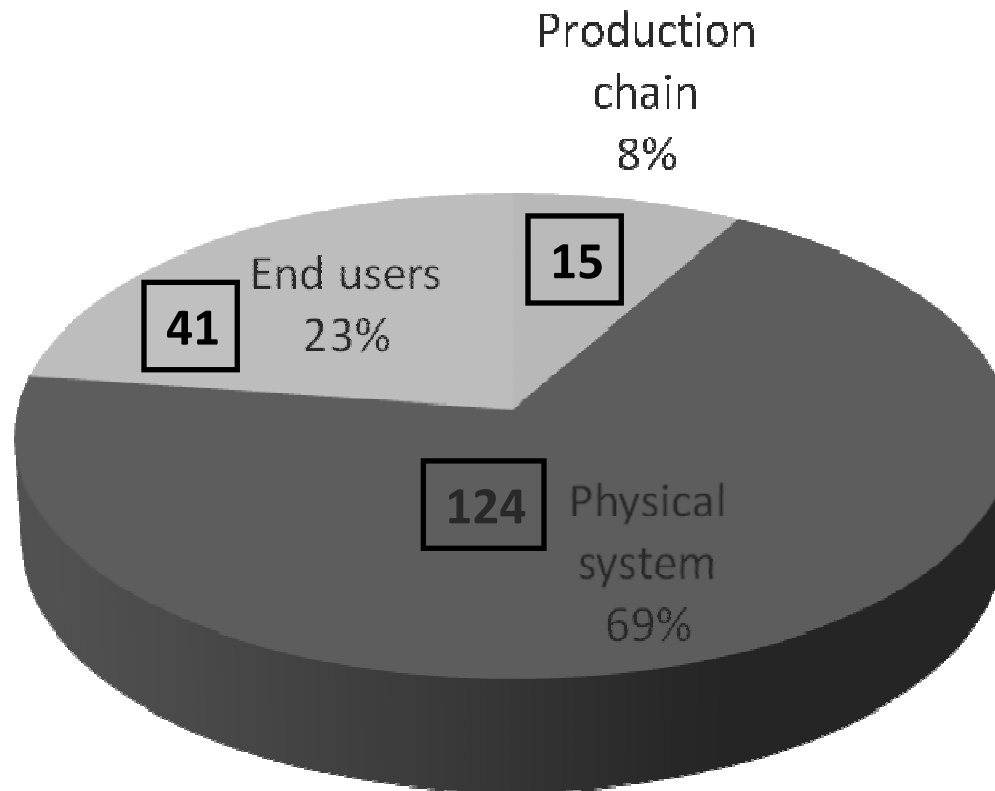
Parties involved in the transformation of ISO/IEC 27001/27002 (Cont.)

- Drafting Committee of GB/T 22080/22081
 - CESI: China Electronic Standardization Institute - Research
 - 30wish: Shanghai 30wish Information Security Co., Ltd. - Product Chain
 - PKSEC: Peking Knowledge Security Engineering Center - Research
 - BJSEC: Beijing Information Technology Security Evaluation Center - Inspection
 - BJCA: Beijing Certificate Authority - Inspection

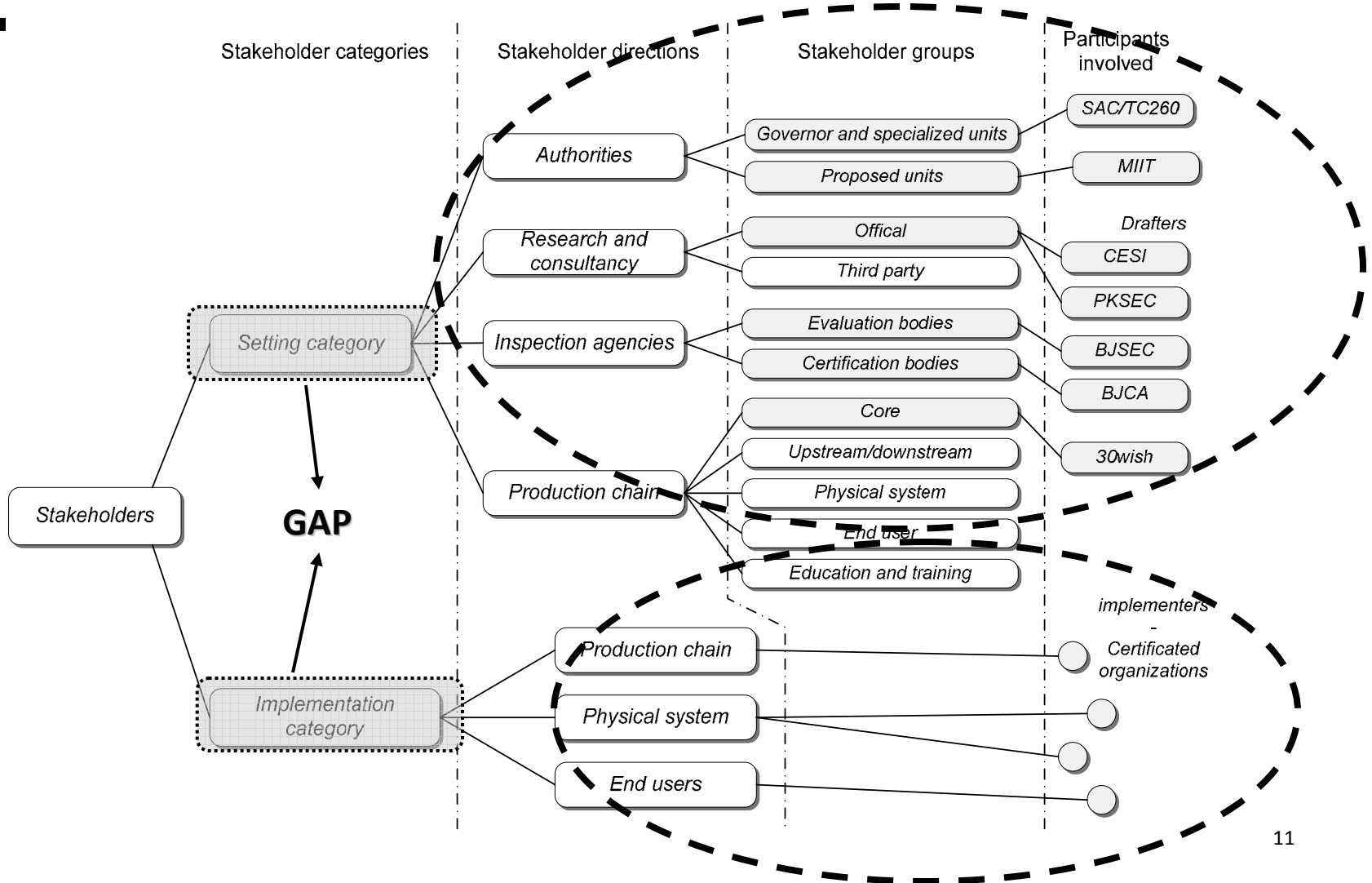
Parties involved in the implementation of ISO/IEC 27001/27002

- Top list of the ISO/IEC 27001 certificates
 - Hardware/software manufacturers (57%)
 - China branches of international enterprises (17%)
 - ISMS production chain companies (8%)
 - Telecommunications operators (6%)
 - Financial companies (6%)
 - Government departments (6%)
 - etc.

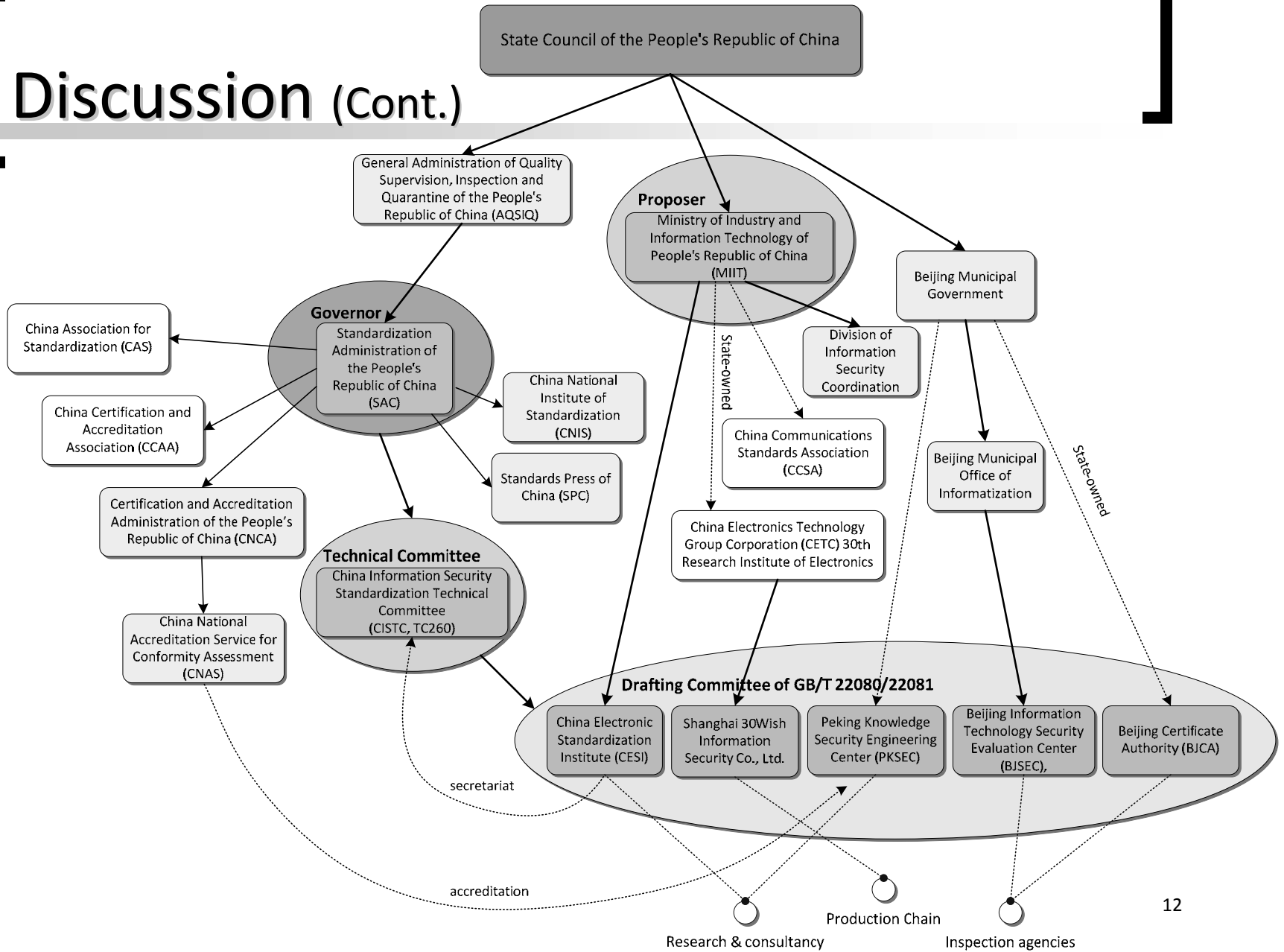
Parties involved in the implementation of ISO/IEC 27001/27002 (Cont.)



Discussion

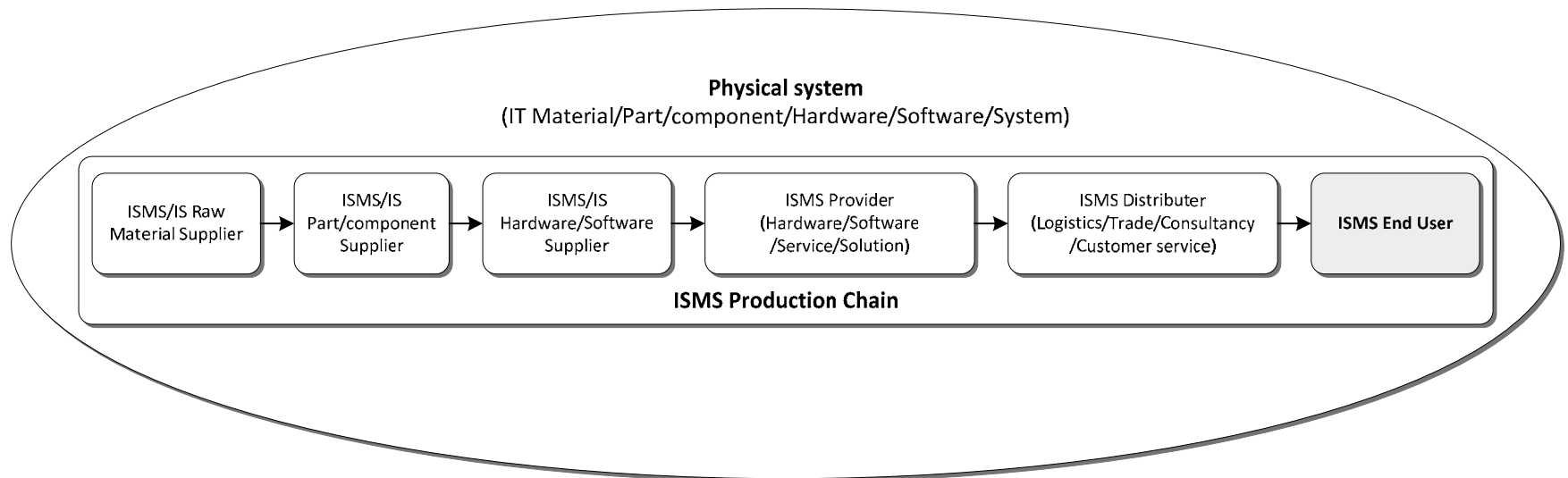


Discussion (Cont.)



Discussion (Cont.)

- The implementation category is in three directions
 - Production chain, Physical system, and other End users



Discussion (Cont.)

- Characteristics of the “early adopters”
 - Leaders in the professional technical field
 - Large-scale enterprises rather than small or medium-sized enterprises (SMEs)
 - Full IS/ISMS or IT/ICT solution abilities
 - With other certificates and qualifications

Conclusions

- The essential participants in standard setting
 - Government authorities
 - Research & consultancy institutions
 - Evaluation & certification bodies
- The participants in standard implementation
 - Physical system companies in the IT/ICT industry
 - End users from government, the financial sector or other sectors
 - ISMS production chain companies

[Policy issue]

- More user participation in the standard setting process?

[Further research]

- More stakeholder analysis
- The business value or ROI of standard users
- The national innovation in ISMS standardization
- The standardization administration system in China

Questions?

■ Xu Yang

- Rotterdam School of Management
 - Erasmus University
 - Rotterdam, the Netherlands
- & School of Management and Economics
- Beijing University of Posts and Telecommunications
 - Beijing, P. R. China
- Yangx.cn@gmail.com XYang@rsm.nl

■ Henk J. de Vries

- Rotterdam School of Management
 - Erasmus University
 - Rotterdam, the Netherlands
 - HVries@rsm.nl