Compositionality of Control

Objectives

Joris Hulstijn (jhulstijn@uvt.nl)

Based on many conversations with Ype van Wijk (Rijksuniversiteit Groningen)
Observations:
(1) Companies create value, as part of network organizations.

Existing frameworks for designing and assessing internal controls (COSO, COBIT) are focused on individual enterprise.

Problem
Van Wijk et al 2014
• Something that plays the role of internal controls in chain or network
• Case 1. Logius
  • IT sourcing for government, complex information chains, embedded outsourcing
  • Problem: enforce information security and other quality requirements over entire chain
• Case 2. Custom Compliance and FloraHolland Cooperative
  • Improve supply chain visibility and customa compliance
  • Use pre-arrival data (pro-forma invoice, phytosanitary certificate) to speed up customs clearance at airport.
  • Problem: physical security and data (integrity of goods flow), data representation standard, business case, governance
Ype’s solution: transfer control obligations

- Internal controls in a chain:

Van Wijk et al 2014
Ype van Wijk (ctd)

- CANTOR framework ©
  - Chain Policy
  - Transference of Obligations Risk-controls (TORC),
  - Chain Internal Control System (CICS)

Van Wijk et al 2014
Essential assumption:

- (1) all chains or network organizations can be understood as a collection of relationships between parties.
- (2) internal controls can be distributed over the network parties, and be integrated to achieve network control objectives.

- Is this true? Are control objectives compositional?
- Under what circumstances?
• **Linguistics:** meaning of a complex expression, depends (solely) on the meaning of its components, and the way it is composed.

  John loves Mary
  NP  TV  NP
  VP   
  S

• **Compositional semantics:** grammars provide syntactic structure, which guide the calculation of the semantics of an expression.

• NB. Only way to understand complexity of human language!
• **Network organizations**: a property of a complex organization, depends (solely) on that property for the components, and on the way it is composed.

\[
P \rightarrow R \\
\neg R
\]

All \((P \lor Q) \implies R\)

Some \(Q \implies \neg R\)

• **Compositional control theory**: graphs provide organizational structure, which will guide calculation of network properties

• NB. Only way to understand complexity of modern business!
Analyzing compositional controls

• **Needed:**
  • Network structure: directed acyclic graphs $G = <N, E>$
  • Representation of properties: proposition logic with labels
  • Composition rules: $n_1 : P_1, \ldots , n_n : P_n \Rightarrow (a_1, \ldots, a_n) : P$ nodes
    
    $all, some$  $e_1 : P_1, \ldots , e_n : P_n \Rightarrow (a_1, \ldots, a_n) : P$ edges

• **Example.** Imagine a blockchain ecosystem for trade data. Certainty about whose goods are where gives financial advantage. Ecosystem maintains identity of owners of goods, and of those who have custody over goods, at all times. So, ecosystem needs to ensure identification and authentication of blockchain members.
Network Organizations

- Network topologies
  - Centralized
  - Peer to peer
  - Cooperative

- Coordination Mechanisms (Malone & Crowston 1994; Ouchi)
  - Hierarchies
  - Markets
  - Clans
  - Delegation
  - Transaction
  - Trust

- Inter-organizational Information systems (IOS)
  - Steinfield et al (2011) IOS structures: coordination hub
  - Crucial: who maintains the representation standard
Network Organizations (ctd)
• **Definition:** “Internal control is a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations” (COSO 1992)

• **Periodic evaluation:** Plan-do-check-act, where check means risk assessment, and act means to implement control measures.

• **Coherent system:** hierarchy of dependencies between control measures, and control measures and control objectives (like in RE)
System of Internal Controls (ctd)

- **Elements** (COSO 192)
  - Control Environment
  - Risk assessment
  - Control activities
  - Information and Communication
  - Monitoring

- Can these elements be de-composed and distributed?
  - Do they apply to all or some partners?
    - all: id & auth
    - some: insurance
Examples

- Can these controls be de-composed and distributed? All or any?
  - data collection immediately at the source,
  - segregation of duties,
  - maintaining an audit trail,
  - access control,
  - baseline security,
  - back-up and retrieval,
  - supervision and monitoring,
  - corporate culture
  - ...
• **Governance:** Thee lines of defense (IIA 2013)
• Depends on coordination mechanism (hierarchy, market, clan)

Can these roles be distributed?
It does make sense to have network-level controls.
Many control objectives are compositional, and can be distributed, using two composition logics: all and some.
Not all control objectives are compositional; in particular, policy-related controls are not, and infrastructure-related controls are not.
An effective network control system would consist of four elements:
- mechanism to decompose a network control objective into controls and if possible distribute them among partners (TORC),
- remaining inherent network level controls (CICS),
- governance structure and business model, to distribute the benefits and costs of investing in network level controls (policy)
- inter-organizational information system (IOS) to share data and monitor effectiveness of controls
Bibliography


As an aside: cyber-physical systems …?

- NSF “Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computation and physical components. Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability that will expand the horizons of these critical systems.”

- Mathematical machinery: aligning graphs
- Could be useful. Need to look into it.
Does it make sense to have a mechanism that plays the role of internal controls, for a network organization?

- Customs compliance: ensure reliability of reporting
- Blockchain ecosystems: trust data on the blockchain
- Embedded outsourcing: guarantee quality for client of client
- Platform Economy: enforce minimal standards

If so, how much and which of the network-level controls can be distributed to the parties that make up the network?

- If so, what are necessary preconditions?
- In other words: are control objectives compositional?