Ministry of the Interior and Kingdom Relations

Cloud Security Standardisation & Certification

Arjan de Jong

Policy Advisor Information Security

Overview

- Economics of standardization and certification
- (EU) Legal requirements for (cloud) security
- International cloud context
- Dutch cloud context
- Conclusion

Economics of information security

- Nature of information security: the act of providing goods or services in the field of information security and not so much the outcome. After a security breach, it does not mean the information security service or product has not been delivered. (Thaw 2011)

- Market mechanisms (and failures) concerning information security
  - Kox & Straathof (CBP; 2013)

Economics of (cloud) security standardization and certification

- Information asymmetry
  - Adverse selection
  - Moral hazard
- First-mover disadvantage
- Transaction costs

Based on Kox & Straathof 2013

- Possible solutions to counter:
  - Information asymmetry
    - Certification
    - Minimum norms of security
    - Security breach notification requirements
- First-mover disadvantage
  - Coordination (with timetable)
- Transaction costs
  - Standardized SLAs

Based on Kox & Straathof 2013

Information Security Regulation

- Main categories of legal requirements
  - Technical measures
  - Organizational measures
  - Notification requirements (conditional)

Based on Thaw 2011

Information Security Regulation

- Information Security Production Lifecycle
  - Planning stage
    - Security / privacy by design
- Implementation and Maintenance stage
  - Procedures, implemented measures
- Output stage
  - Information security itself is the output, which can be present at all stages of the lifecycle
    - Regulation targeted at the outcome stage can influence other stages in the lifecycle.
      - E.g. Notification is only required when personal data is not encrypted.
        - Result: controllers are given the incentive to encrypt their data, influencing the implementation and maintenance stage.

Based on Thaw 2011

(EU) Legal requirements for (cloud) security

Personally Identifiable Information (PII)

- Directive 95/46/EC
  - Article 17 (1)
    - Controller must implement appropriate technical and organizational measures
    - With regard to the state of the art and the costs of implementation, it will have to ensure a level of security appropriate to the risks represented by the processing and nature of the personal data.
    - Risk based
  - Article 17 (2)
    - Controller has to ensure that processor also complies and takes sufficient technical and organizational measures

Dutch Data Protection Authority

- Guidance on securing PII (2013)
  - ISO 27001/27002
  - Web application guidelines National Cyber Security Centre
  - Sectoral guidelines (NEN 7510; Healthcare)

Proposed General Data Protection Regulation

- Article 23 (privacy by design and default)
  - (1)
    - Having regard to the state of the art and cost of implementation
    - At the time of the determination of the means of processing and at the time of processing itself
    - Implement appropriate technical and organisational measures
    - To meet the requirements of the regulation
  - (2)
    - Restrict processing to personal data necessary to achieve the specific purpose
    - Do not collect or retain more personal data beyond the minimum necessary to achieve the specific purpose

Proposed General Data Protection Regulation

- (4) The Commission may lay down technical standards

Proposed General Data Protection Regulation

- Article 30
  - Comparable to article 17 Directive 95/46/EC
    - (1) The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
    - (2) Measures have to be taken based on a risk evaluation
- Demonstration of compliance? Role for certification or codes of conduct?

- Article 31 Data breach notification to supervisory authority
  - (1) In case of a data breach the controller has to inform the supervisory authority without undue delay
  - (2) Processor has to alert and inform the controller immediately after establishment of a data breach
  - (4) Documentation of breach
  - (6) Standard forms for notification

- Article 32 Data breach notification to the datasubject
  - (1) Controller has to inform the datasubject without undue delay when the personal data breach is likely to [adversely/severly] affect the protection of the personal data or privacy of the data subject
  - Give details on data protection officer and possible measures to mitigate negative consequences to the data subject
  - Notification not required when appropriate technical measures have been taken. (e.g. adequately implemented encryption)

Non-PII specific

- Proposed Network and Information Security Directive (NIS)
  - Requirements for market operators and public administrations
    - Article 14 (Security & notification requirements)
      - Public administrations and market operators have to take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations.
      - Risk based
      - Notification required to competent authority of incidents that have a significant impact on the security of their core services
- Article 16 (Standardisation of network and information security)
  - Member States shall encourage the use of standards and/or specifications relevant to network and information security

European Cloud Strategy

- Cutting through the jungle of technical standards
- EU-wide certification schemes for trustworthy cloud providers
- Development of 'safe and fair' contact terms/SLAs
- European Cloud Partnership / Cloud for Europe

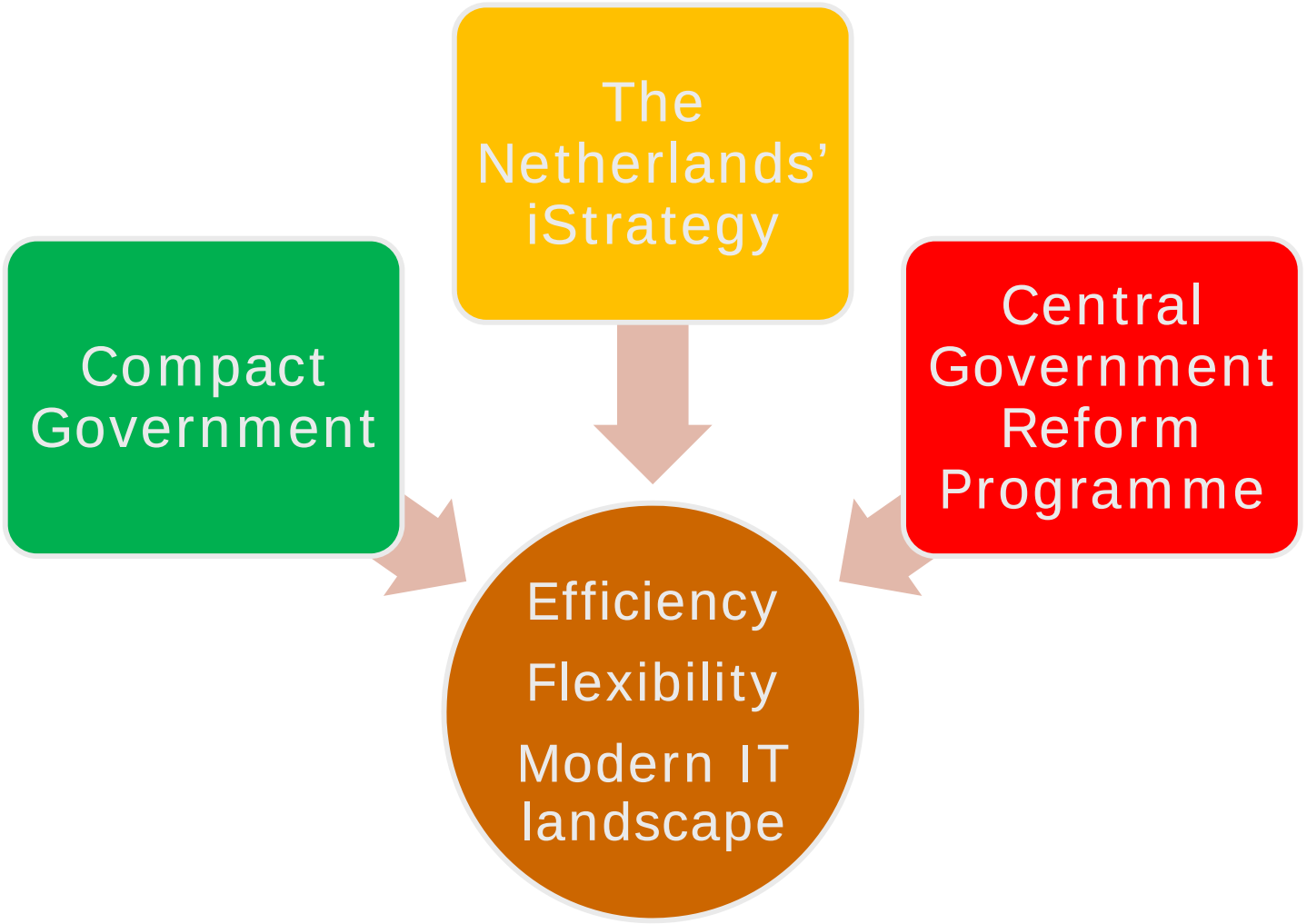
International developments

- European Cloud Partnership
  - Steering board meeting Tallinn Estonia, 4 July 2013
- Cloud for Europe
  - Cloud for Europe Conference Berlin, 14-15 November 2013
- ENISA Cloud Security WG
  - Top 10 recommendations for deploying Governmental clouds
- ETSI Cloud Standards Coordination
  - (Draft) Final Report, November 2013
- Opinion European Parliament Committee on Legal Affairs on EU Cloud Strategy
  - Calling for voluntary cloud certification (23 september 2013)

Dutch context

- Dutch Government reform program
- Dutch Governmental Cloud Strategy
- Dutch Standardization Policy

Dutch Government Reform Program



Dutch Governmental Cloud Strategy

1 First phase is building a **Closed Government Cloud (CGC)**

2 Next phases **growth in use and cloud offerings**

3 **Cloud First Strategy**

Dutch Governmental Cloud Strategy

- Closed Governmental Cloud (CGC)
- Challenges
  - Security
  - Interoperability
  - Data portability
  - Reversibility
  - Governance
- Functional goal architecture
  - Approved June 27 2013 by the Board of CIOs from Central Government

Functional goal architecture

- Topics addressed:
  - Datacenters; new Government network; Government Application Store; Government Workplace as a Service (DAAS)
  - Selfservice
  - Finance; pay per use
  - Identity Management
  - Data protection
  - Cloud resources
  - Connectivity
  - Cloud Governance
  - Cloud Standards

Dutch Standardization Policy

- Netherlands Openly Connected (-2011)
- Forum Standardisation
- List of open standards (public procurement)
  - Apply or explain list
    - e.g. DKIM, DNSSEC, ISO 27001/27002, SAML)
  - Recommended open standards
    - e.g. OAUTH, XML

Questions?

Contact:
Arjan de Jong, LLM
Policy Advisor Information Security
Arjan.Jong2@minbzk.nl

Ministry of the Interior and Kingdom Relations, The Netherlands
www.government.nl