Waarom deelnemen aan standaardisatie?

Mirna Bognar, ING Bank

Amsterdam, 12 December 2017

"The good thing about standards is that there are so many to choose from."

— *Andrew S. Tanenbaum*

ING

Wet- en regelgeving, standaarden en normen: hoe werkt het

- E.g. General Data Protection Regulation (GDPR)
  - Hoe GDPR te implementeren?
    - E.g. Guidelines on Data Protection Impact Assessment (DPIA) door Article 29 Working Party
    - E.g. ISO standaarden over Data Privacy Architecture
    - E.g. interne “minimum standaarden”, richtlijnen
- Standaarden en normen geven een houvast

As an IT security professional
I want to be informed and to understand

ING

Wet- en regelgeving, standaarden en normen: ook faciliterend

- E.g. Obama's Executive Order Improving Critical Infrastructure Cybercrime Feb 2013
  - *It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards.*

- NIST Framework for Improving Critical Infrastructure Cybersecurity

- Information Sharing and Analysis Centres (ISACs)

As an IT security professional
I want to collaborate

ING

Wet- en regelgeving, standaarden en normen: de uitdagingen

- E.g. General Data Protection Regulation (GDPR)
  - Rol van CISO
- E.g. Basel Committee of Banking Supervision en *Three lines of defence*
  - Three lines of defence genoemd als best industry practice.
    Wel wordt er geaudit t.o.v. three lines of defence
- E.g. PSD2
  - Veel discussies gaande
- Informatiebeveiliging vs. privacy?
  - US: security boven privacy
  - EU: privacy boven security

As an IT security professional
I want to contribute and steer

ING

Wet- en regelgeving, standaarden en normen: Waarom meedoen?

- Volgen
- Begrijpen hoe toe te passen
- Bijdragen
- Stem uitbrengen

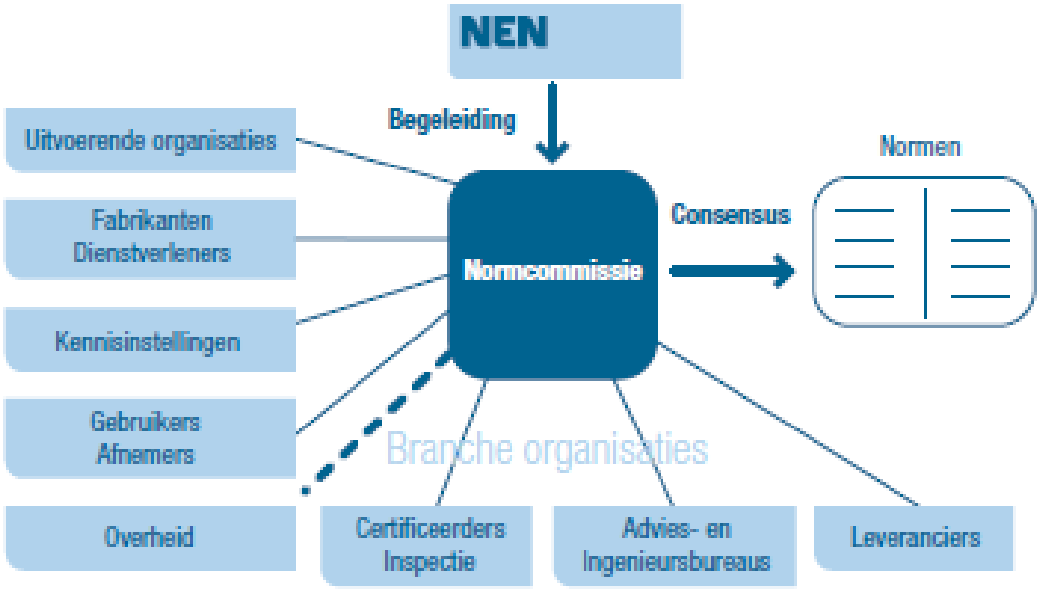
As an IT security professional
I want to be informed and to understand

As an IT security professional
I want to collaborate

As an IT security professional
I want to contribute and steer

Wat kan ik als deelnemer van een werkgroep van NEN verwachten?

1. Toegang tot een groot (internationaal) netwerk
2. Vroegtijdige kennis van de normen die gaan komen
3. Invloed op de normen
4. Begeleiding door NEN (procedureel, welke norm wel en niet maken, begeleiding bij zelf initiatief nemen voor een norm)
5. Draagvlak creëren



Uitnodiging: Er is standaardisatie gaande…

- Informatiebeveiliging in *Agile Way of Working*
  - Concreter maken van de normen d.m.v. *Use cases*?
  - Aanpassing van ISO 2700x nodig? E.g. Segregation of Duties

- GDPR: verdere verduidelijking nodig?

- Met het tempo van innovatie en *end2end* ketenafhankelijkheden, is de verwachting dat de behoefte naar afspraken en normen zullen toenemen

Ga naar mentimeter

www.menti.com

23 32 03

Dank u voor uw aandacht