Conformity assessment and standards

EEMA 2017, July 5, 2017

Andrew Hughes, CISM CISSP
Leadership Council Chair, Kantara Initiative
KantaraInitiative.org
The Kantara Initiative is the global consortium improving trustworthy use of identity and personal data through innovation, standardization and good practice
Today’s Topics

- The elements of Conformity Assessment Systems

- Use of standards and conformity assessment to evaluate promised services as ‘fit for purpose’ and ‘meets expectations’

- The meaning of Codes of Conduct and Certification for GDPR compliance

- Principles and Value of Open Standards
PROBLEM: GAINING TRUST IN PROMISED SERVICES

- What do you & your organization look for in online products and services to believe they are trust-worthy and are a solid solution?

- How can a commercial reputation for quality be expressed?

- How can GDPR compliance be demonstrated?
Some Possible Solutions

- Use recognized standards to develop and deliver services

- Undergo conformity assessment and obtain a licensed Mark of conformity as evidence of conforming to specified standards such as Codes of Conduct

- Negotiate contracts (unilateral, bi-lateral, multi-lateral)

- Purchase services that display the desired Mark of conformity
**SOME CONCEPTS**

- **Standards** are a consensus on how an activity *should be done* or a product made. They should be developed using open, transparent, voluntary processes.

- A **Mark of Conformity** represents a *commitment* by the licensee to achieve specified quality as defined in a standard.

- **Conformity Assessment** is used to evaluate how an activity *is actually being done* (and may result in issuance of a licensed Mark).
A Scenario

SHOEME.COM AND PERSONAL DATA PROTECTION RISKS
THE SCENARIO

- Overall scenario – online retail based on personal information and preferences
- Problem – each participant is at risk if the other is a bad apple or careless
- Solution – What do you do in real life?
  - get information about track record
  - determine if good practices are used
- How is this possible in the online world?
SCENARIO – SHOE ME.COM

S. Shopper

Gives personal information for custom store recommendations

ShoeMe.com
SCENARIO – SHOEME.COM

S. Shopper

Gives personal information for federated authentication services

Gives personal information for custom store recommendations

myLogonFriend.com

ShoeMe.com

Use secure authentication protocol for federated single sign-on

© Copyright 2017 Kantara Initiative, Inc.
SCENARIO – SHOE ME.COM

Do ShoeMe and myLogonFriend protect information well? Are they using good industry practices? Is my information safe?

Does ShoeMe protect information well? Do they comply with GDPR?

Does myLogonFriend protect information well? Do they comply with GDPR?
SCENARIO – SHOE.ME.COM

Use Conformity Assessment to assess whether the organizations meet the requirements as stated in standards!
DEFINITION: CONFORMITY ASSESSMENT

- Conformity assessment: demonstration that specified requirements relating to a product, process, system, person or body are fulfilled (ISO/IEC 17000:2004)
The Value of Conformity Assessment

- Undergoing the conformity assessment process has a number of benefits:
  - It provides consumers and other stakeholders with added confidence.
  - It can give your company a competitive edge.
  - It helps regulators ensure that health, safety, environmental conditions, security and other requirements are met.
ISO/IEC 17000 ‘FUNCTIONAL APPROACH’

- ISO/IEC 17000
  *Conformity assessment – Vocabulary and general principles*
- Part of a family of standards on Conformity Assessment
- ‘Functional Approach’ is proposed
  - Selection – choose the standard; decide on sampling & techniques
  - Determination – testing, inspection, auditing, examination
  - Review & Attestation – decide on conformity to the specified requirements; issue statement of conformity; issue a Mark
  - Surveillance – monitoring out in the marketplace
WHAT IS A MARK OF CONFORMITY?
**Mark of Conformity**

- A Mark of conformity is an indication that an organization has demonstrated conformity to standards which set expectations of quality.
- A Mark of conformity may be licensed to qualified organizations.
- The license contains terms and conditions to have the right to use the mark – e.g. the licensee must remain in conformity.
WHY TRUST A MARK ISSUER?

- A Mark issuer conforms to standards (of course). The issuer uses a formal conformity assessment system to ensure the quality of the licensee’s products and services.

- Mark issuers should be Accredited: evaluated by peers to confirm quality of the conformity assessment scheme and Mark license.

- Accreditation increases the value of issued Marks.
WHAT IS A SYSTEM OF CONFORMITY ASSESSMENT?

- Conformity assessment system: rules, procedures and management for carrying out conformity assessment

(ISO/IEC 17000:2004)
CONFORMITY ASSESSMENT SYSTEM

Standards

Conformity Assessment System

Conformity Attestation & Certification

Assessment Scheme Rules

Mark of Conformity

Qualified Assessors
WHO PERFORMS ASSESSMENTS?

● 1\textsuperscript{st} Party Assessment = Internal Independent Assessor
● 2\textsuperscript{nd} Party Assessment = A Supplier requirement
● 3\textsuperscript{rd} Party Assessment = External Independent Assessor

● Significance
  ● There is high value in each type of conformity assessment; 3\textsuperscript{rd} party assessment (certification) is not always required
Examples of

CONFORMITY ASSESSMENT SCHEMES
The Kantara Identity Assurance Assessment Framework

- Assess fulfilment of requirements of NIST SP 800-63 v2 or equivalent standards (Credential Management, Identity Proofing, Credential Authentication)
- Kantara Initiative manages the scheme: the assessment rules, approval processes and assessment criteria
- Kantara Initiative licenses marks of conformity
- Currently developing a scheme to assess conformity to NIST SP 800-63 v3
A (NEW) CONSENT SYSTEM ASSESSMENT SCHEME

- Kantara is developing requirements around best current practice for systems that collect an individual’s consent to share data
  - Designed to meet GDPR requirements at minimum
  - Should be applicable to any FIPPs-oriented regulation
  - New WG starting July/August
  - Expect drafts around December 2017
  - Could lead to development of Code of Conduct and/or Certification for GDPR
INFORMATION SECURITY MANAGEMENT SYSTEMS

- ISO/IEC 27001: Information technology — Security techniques — Information security management systems — Requirements
- Requirements for information security management systems
OPEN STANDARDS
Standards provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that [...] processes and services are fit for their purpose.
— www.iso.org
OPEN STANDARDS

- Cooperation
- Adherence to Principles
- Collective Empowerment
- Availability
- Voluntary Adoption
10 Benefits of Open Standards

- Address Market Needs
- Reduce Costs
- Drive Interoperability and Scalability
- Encourage Market Competition
- Leverage Expert Knowledge
A Scenario

SHOEME.COM AND PERSONAL DATA PROTECTION RISKS
CONCLUSION – SHOE ME.COM
CONCLUSION – SHOE ME.COM

myLogonFriend.com

S. Shopper

ShoeMe.com
CONCLUSION – SHOEME.COM
CONFORMITY ASSESSMENT SYSTEM

- Standards
- Assessment Scheme Rules
- Conformity Assessment System
- Conformity Attestation & Certification
- Mark of Conformity
- Qualified Assessors

© Copyright 2017 Kantara Initiative, Inc.
The Kantara Initiative is the global consortium improving trustworthy use of identity and personal data through innovation, standardization and good practice.

Kantara Leadership Council Chair: AndrewHughes3000@gmail.com
General Inquiries: support@kantarainitiative.org
KantaraInitiative.org