IT & Audit in het Volgende Decennium

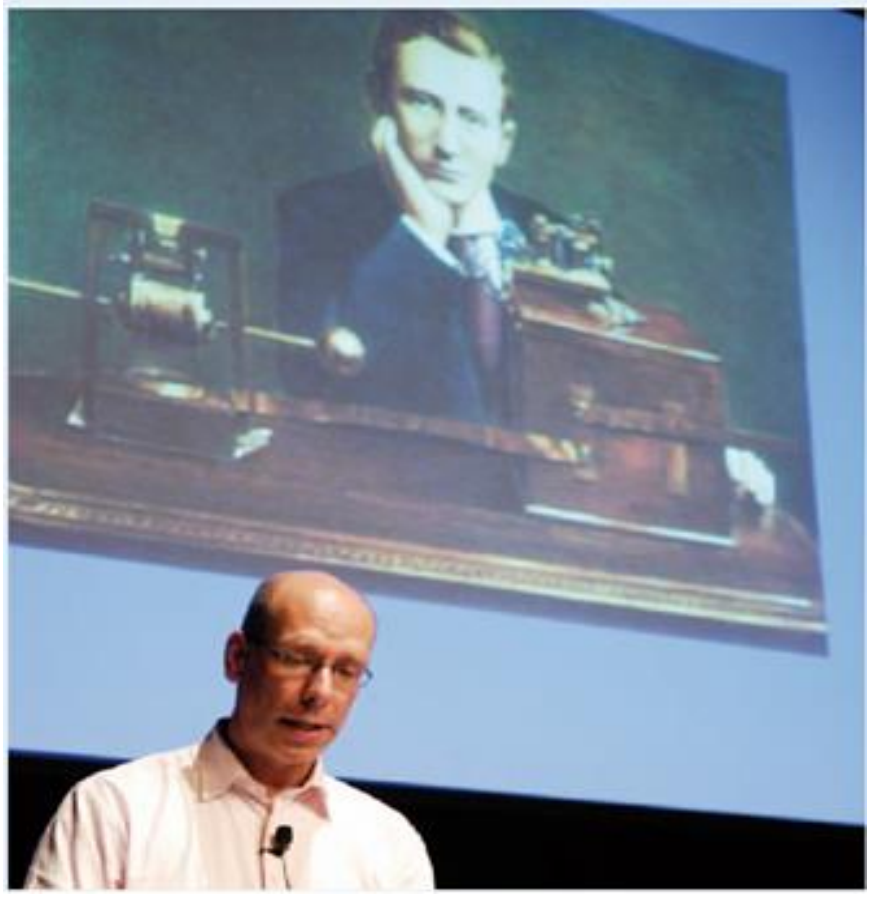
“Verbetert Digital Assurance de relevantie én de kwaliteit van het oordeel van de RE?”

Jan Matto, Mazars

Vrije Universiteit, Amsterdam
14 September 2015

MAZARS

Even voorstellen:



- Partner Mazars (Management Consultants)
  Center of Excellence IT-audit & -advisory

<u>Andere professionele activiteiten</u>:

- Commissie Veilige Verbindingen, EZ,ECP,DHPA
- Commissie “Zeker Online”, Belastingdienst / ECP
- Publicaties over IT audit en IT security
- Colleges voor verschillende universiteiten
- Commissie van toelating / visitatie NOREA
- Stuurgroep Permanente Educatie Register-accountants IT en assurance, Veritas / VERA)

Email: jan.matto@mazars.nl

@Jan_Matto

Voorbeelden van IT audit projecten:

- Onderzoek datalek en informatiebeveiliging NZa
- Onderzoek reeks omvangrijke overheids ICT projecten
- Advies beveiligingsbeleid Politie Nederland
- Onderzoek biometrische gezichtsherkenningsystemen grensbewaking (No-Q)
- Privacy en security certificering Fraude detectiesystemen
- Privacy Impact Assessment identity management systemen (eID Stelsel)
- Privacy en security audit Electronische Nederlandse IdentiteitsKaart (eNIK)
- Assurance services voor IT Service Providers
- Third Party Rapportages, ISAE3402 audits en DigiD Assessments
- Mediation IT projecten / project recovery / calamiteiten

Wat beoogt Digital Assurance?

- Geeft inzicht in de toestand van het reële ICT systeem: “De IT werkelijkheid”;
- Via waarnemingen in de IT werkelijkheid;
- Waarnemingen vinden plaats op verschillende systeemniveaus / -lagen
  - *Architectuur, inclusief ketens, cloud en onderliggende systeemlagen (onderkent dat systemen veelal via netwerken gekoppeld zijn / vervaagde systeemgrenzen)*
  - *Uitrusting en inrichting;*
  - *Events en violations in systemen;*
  - *Transacties, reguliere processen, data.*
- Inzet van tooling is daarbij belangrijk;
- Gaat meer in de richting van monitoring, detectie en respons;
- Normen te ontlenen uit de actuele context van het IT systeem;
- Rapportage / transparantieverslag over systeem functioneren.

Setting the scene: IT en “The Loss of Governance”

Toenemende Complexiteit / distributie

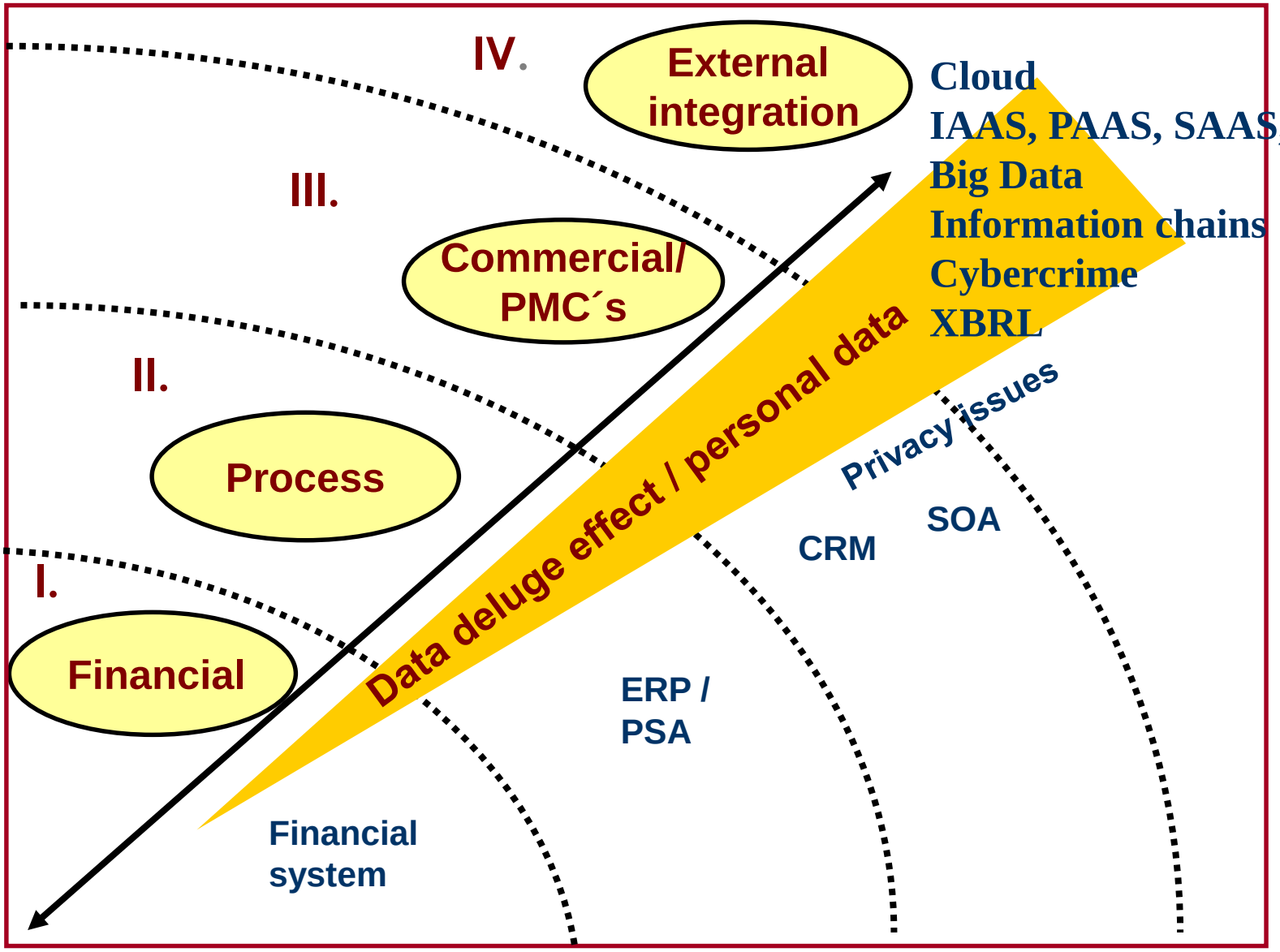
Systeem technische overgangen

Verschuivingen in dominante macht

Verschillen in compliance

Meer frequente system changes

Toename risico’s:
- Strategische rol IT
- Afhankelijkheid van beschikbaarheid IT
- Information chains
- Vitale infrastructuren
- Cyber security risks
- Ontstaan “hotspots”…..
- Surveillance en “the Man in the Middle”
- Aanscherping wet- en regelgeving
- ……



Kleine verdieping achtergrond IT Audit en Digital Assurance:

Traditionele audit benaderingen (main stream)

- ➔ Beheersdoelstellingen, risico's, beheersmaatregelen, stabiliteit
- ➔ Rule based = "harde" normen en maatregelen
- ➔ Principle based = formulering van beheersdoelstellingen

Noodzaak tot meer geavanceerd IT auditeren

- ➔ Context based
  - ➔ *De context zet de norm*
  - ➔ *Als de context verandert kloppen principles en rules wellicht niet meer*
  - ➔ *Een IT systeem zou vooral:*
    - A) een "afbeelding" moeten zijn van haar context
    - B) dus moeten kunnen anticiperen op haar context

- ➔ Digital Assurance focust meer op de systeem context en IT werkelijkheid

Drivers voor Digital Assurance: nieuw gedrag door stakeholders ten aanzien van IT

Journalists

Autoriteit Consument & Markt

Regulators

Government

Privacy regulators

Citizens, Consumers, Society

Politics

Hackers

ANONYMOUS

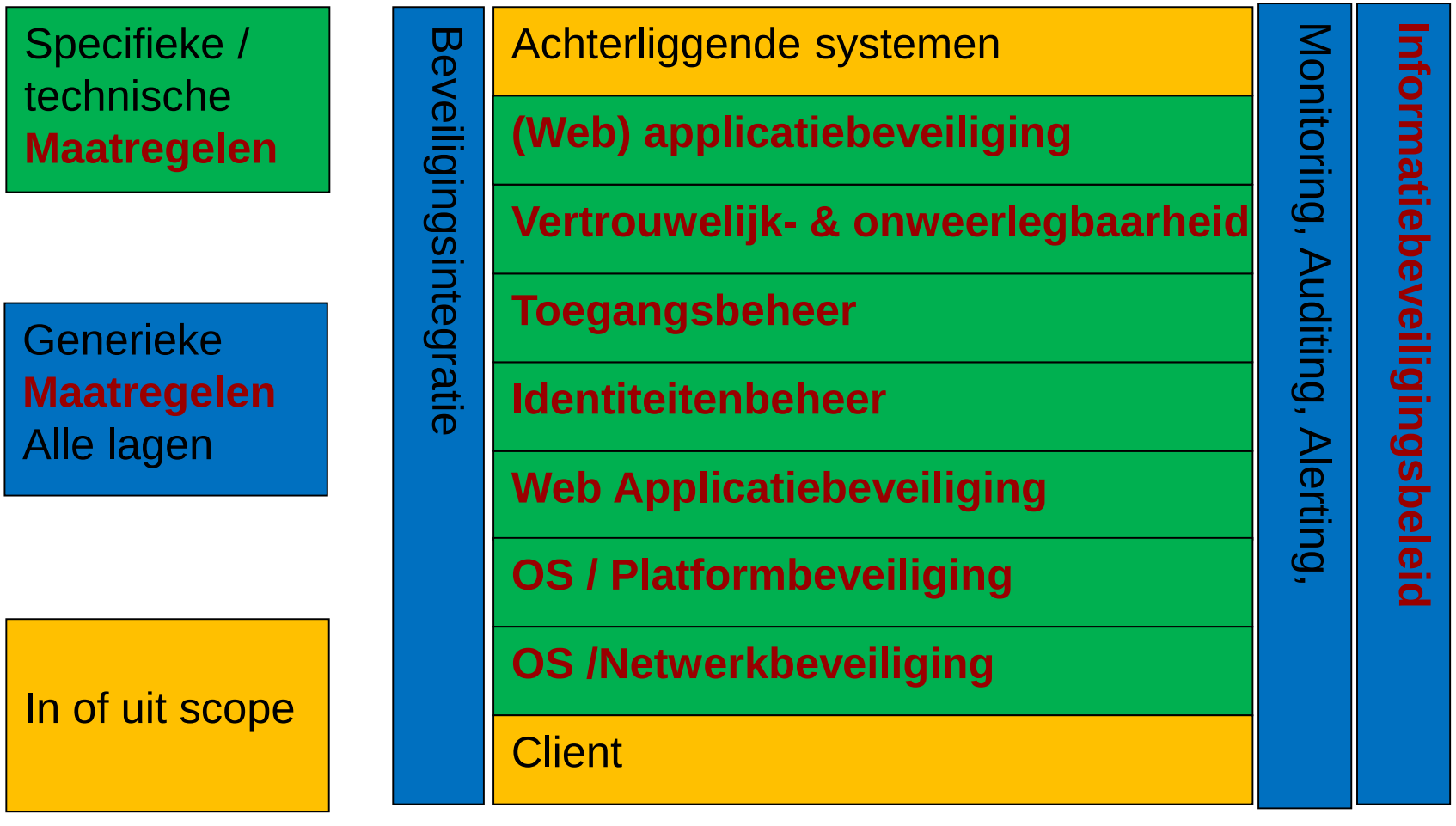
Civil rights & privacy protectors

Bits of Freedom

➔ Kritisch blik van derden op uw IT Architectuur & Services
➔ en indirect dus ook op IT audit bevindingen en rapportages

Digital Assurance: hoe werkt het?

Onderkennen dat een ICT systeem uit verschillende lagen en schakels bestaat en even zoveel ingangen heeft en verschillende audit-kijkniveaus heeft.



Voorbeeld Digital Assurance: Logische toegangsbeveiliging (1)

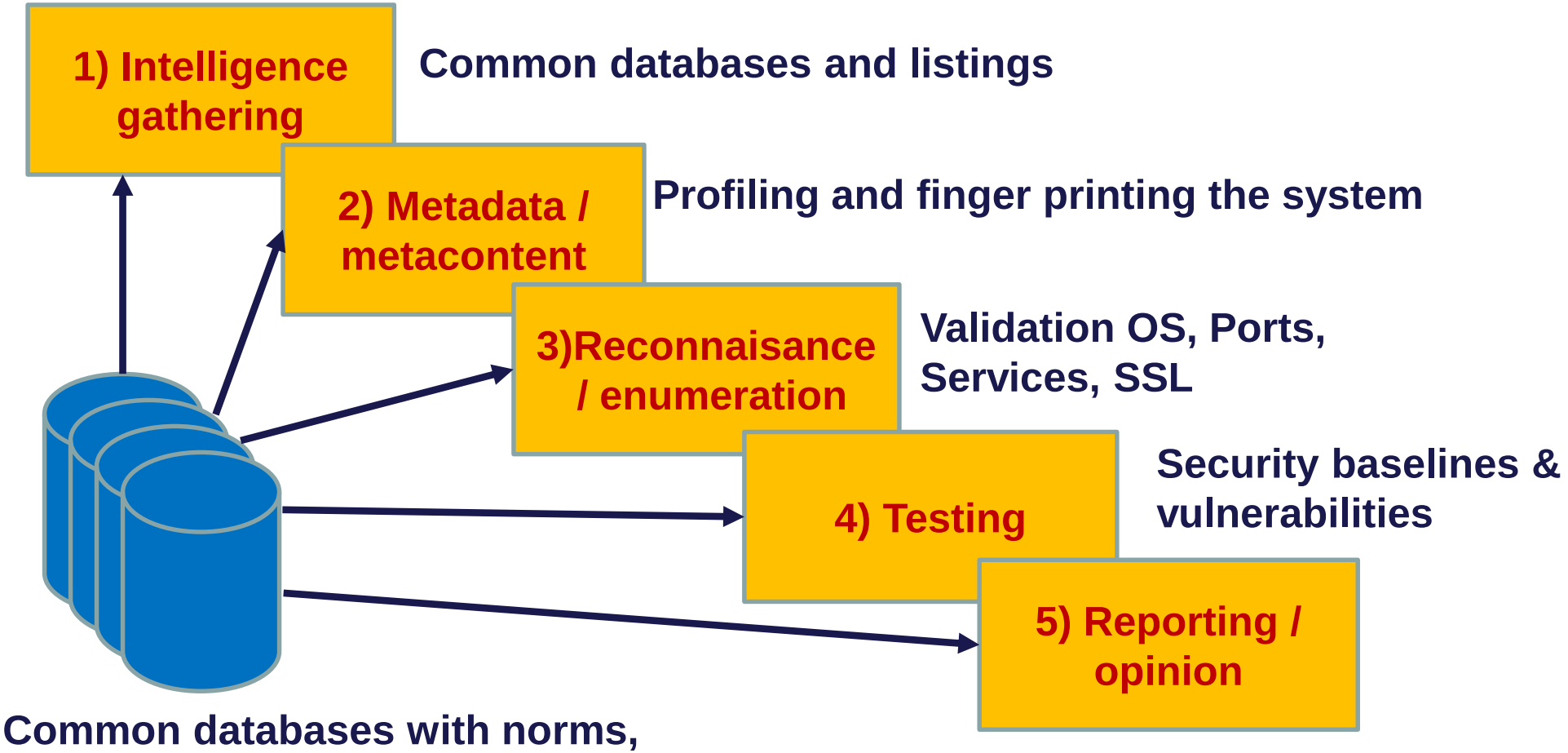
1) **Intern: netwerk en besturingssystemen / platform**:

Netwerk en architectuur zijn bekend en van binnenuit bereikbaar.

- Verkenning en scanning van netwerk en architectuur;
- Uitlezen van security instellingen gevonden objecten;
- Uitlezen van logfiles, sporen, violations, etc.
- Scannen van kwetsbaarheden en instellingen van binnen netwerk aanwezige objecten;
- Confrontatie met bevindingen ITGCs, procedures, informatiebeleid, contractuele afspraken etc.
- Rapportage van bevindingen (opinie over accountmanagement, logische toegangsbeveiliging, incident management, patch management, etc).

Voorbeeld Digital Assurance: Logische toegangsbeveiliging (2)

2) **Extern: Webapplicaties, URLs, IP reeksen**



Voorbeeld Digital Assurance: Logische toegangsbeveiliging (3)

2) **Extern: Webapplicaties, URLs, IP reeksen**

1) Intelligence gathering

A) Intelligence gathering / common listings

- Website en webapplicatie
- Reputation (oa. via openbare “common” data bases)

  Risk rating

  Block lists / black lists

  Web reputation / Malware

  Indicatie van incidenten

Voorbeelden: Netcraft, Google, Senderbase en vele anderen

Voorbeeld Digital Assurance: Logische toegangsbeveiliging (4)

2) **Extern: Webapplicaties, URLs, IP reeksen**

2) Metadata / metacontent

B) Metadata / metacontent

- Functioneel aflopen website / webtoepassing / webforms / documents / etc
- Profiling the system / finger printing
- Authors, creators, time, date, standards, accountnames, email, locations, etc
- Software in use, internal network information, etc.

Voorbeeld Digital Assurance: Logische toegangsbeveiliging (5)

2) **Extern: Webapplicaties, URLs, IP reeksen**

3)Reconnaisance / enumeration

C) Reconnaissance / enumeration

- OS identification
- Port and Services identification
- SSL Analysis

Voorbeeld Digital Assurance: Logische toegangsbeveiliging (6)

2) **Extern: Webapplicaties, URLs, IP reeksen**

4) Testing

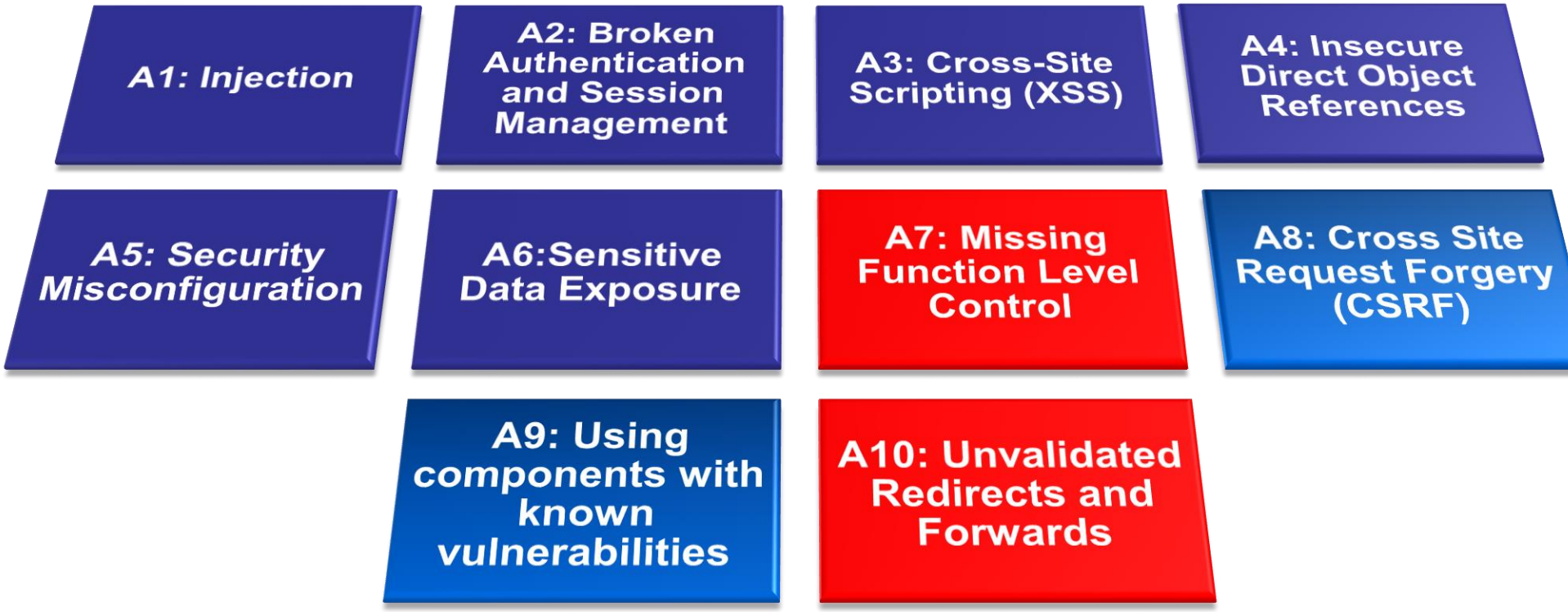
D) Testing security / logical access

- Vaststellen relevante vulnerabilities en testen maatregelen
- Mapping met normenkaders (CVE, CVSS, NCSC, DigiD, OWASP, etc)
  - CVE: Common vulnerability and exposures database
  - CVSS: Common vulnerability scoring system
- Testen hardening / invoer validaties / error trapping / etc
- Evaluatie security parameters / objecten
- Confrontatie met bevindingen ITGCs, procedures, informatiebeleid, contractuele afspraken etc.

5) Reporting / opinion

- Rapportage van bevindingen (opinie over accountmanagement, logische toegangsbeveiliging, incident management, patch management, etc).

OWASP Top Ten 2013



OWASP
The Open Web Application Security Project
http://www.owasp.org

http://www.owasp.org/index.php/Top_10

MAZARS

Verbetert Digital Assurance de relevantie en de kwaliteit van het oordeel van de RE?:

Hoe hard is anno 2015 de koppeling tussen:

(IT) Governance

en

de kwaliteit van een IT systeem?

Drivers voor digital assurance komend decennium

- Aanhoudende stroom aan ICT en security incidenten
- Toenemende maatschappelijke en economische relevantie van ICT
- Toenemende maatschappelijke bewustwording van ICT risico's
- Wet- en regelgeving inzake privacy, data protectie en mededinging
- Toenemende ICT-interdependentie ondernemingen en instellingen
- Toenemende behoefte assurance en transparantie over IT bij uitbesteding
- Ontstaan van nieuwe normen op IT systeemniveau
- Ontstaan van nieuwe initiatieven voor IT assurance en gerelateerde diensten
- Toenemende juridisering en aansprakelijkheidsdenken
- Zichtbare beperkingen van traditionele IT audit benaderingen

Dank voor uw aandacht!

Jan.Matto@Mazars.nl

06 535 78 232

@Jan_Matto

MAZARS

Dank voor uw aandacht