OASIS IDtrust

Processing Cyber Threat Data Through the GDPR Regulatory Lens:

for Operational Compliance with GDPR *and …* Improved Privacy Risk Management

John Sabo, CISSP
Chair OASIS IDTrust Member Section
Chair, OASIS PMRM Technical Committee
john.sabo711@yahoo.com

Special Thanks to Mike Small

kuppingercole
ANALYSTS

GDPR/Privacy Engineering Tutorial

- Eight-part online workshop tutorial recorded at the KuppingerCole European Identity and Cloud Conference 2017 in Munich

- Online on the OASIS YouTube Channel:
  - OASIS Open Standards
- https://www.youtube.com/user/OASISopen/playlists

Privacy Principles – GDPR Article 5

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- **Security** – confidentiality, integrity, **availability and resilience**

Consent - GDPR Article 7

- Controller shall be able to demonstrate that the data subject has **consented** to processing of personal data.
- The request for consent shall be presented in a manner which is **clearly distinguishable** from … other matters …intelligible … easily accessible …clear and plain language.
- Data subject shall have the **right to withdraw** …consent at any time. … It shall be as easy to withdraw as to give consent.

GDPR - Personal Data

- *Any information* **relating to an identified or identifiable natural person**. Specific references to:
  - **identification number**; **location data; online identifier**
- **One or more factors** specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

GDPR – New Regulatory Concepts …

- **Large administrative penalties - up to 4% of annual turnover**
- **Global Scope (directly impacts non-EU organizations)**
- **Both Controller and Processor Responsibilities (cloud implications)**
- **Processors must have documented processing instructions**
- **Rights of Rectification, Erasure, and Restricted Processing**
- **Pseudonymisation (separately maintained additional information)**
- **Data Protection by Design and Default (design + implementation)**
- **Granular Consent and Withdrawal of Consent**

GDPR as Catalyst

Pre-GDPR?

① Primary focus on policy – regulators lawyers

② Security-centric

③ Limited understanding of technical implementations and inter-dependencies

④ Traditional privacy risk management – "PIAs"

Post-GDPR?

① Multi-stakeholder focus

② Holistic "data protection" approach

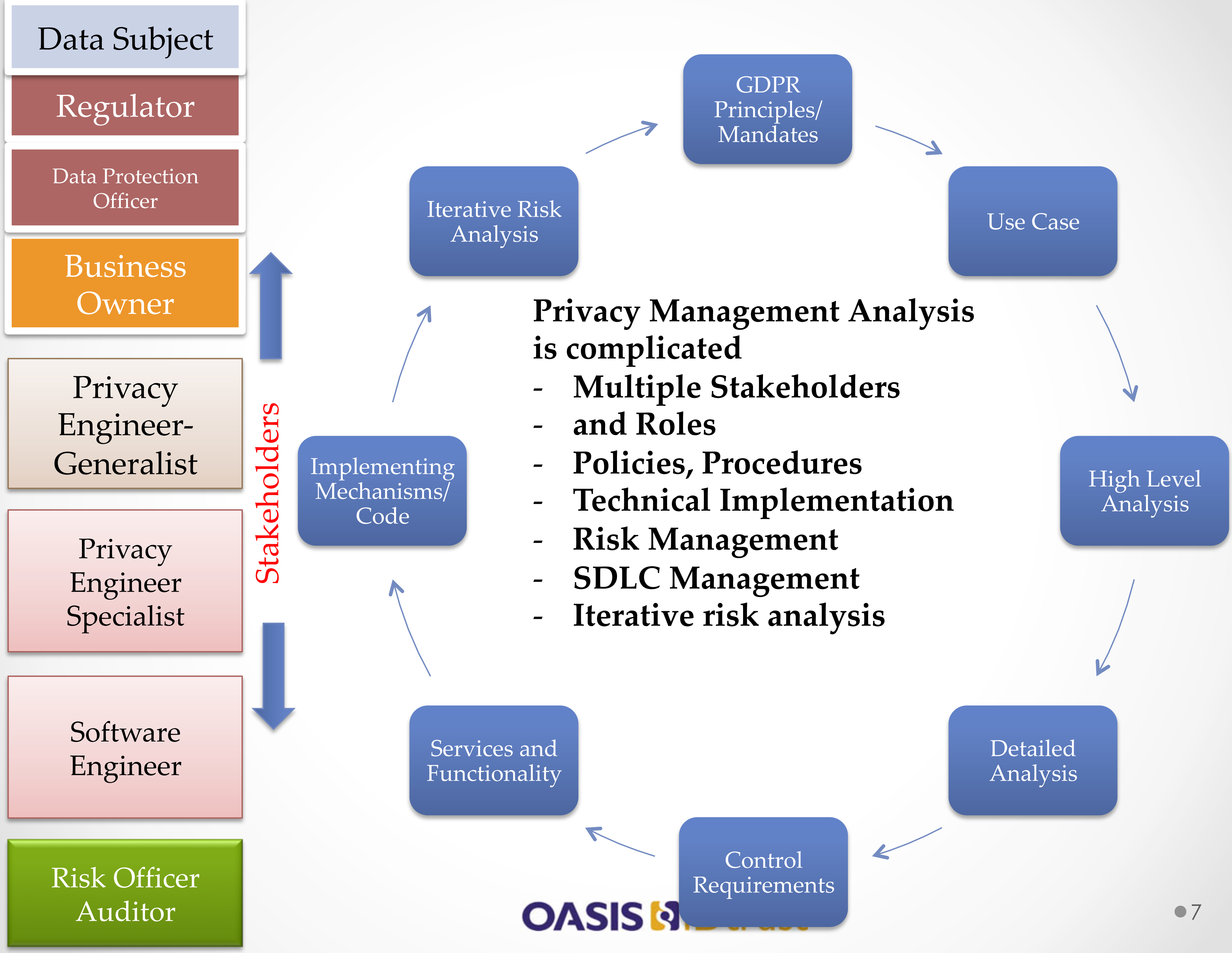
③ Deep understanding of technical implementation and inter-dependencies

④ Proactive risk management – data protection by design and default

How Can the OASIS PMRM Help You Meet the Letter and Spirit of the GDPR in Cyber Security Systems?

- **PMRM V1.0 CS02 – Privacy Management Reference Model and Methodology**
- An **analytic tool**:
  - Enables the **structured analysis of "use cases"** in which Personal Data (or PII) are used, generated, communicated, processed, stored and erased
  - Shows the **linkages** among PII, data flows, data protection [including security] policies, privacy controls, privacy-enabling Services/Functionality/Technical Mechanisms] and Risk Management
  - **Supports any set of privacy standards and policies**
  - Supports **Data Protection by Design requirements and compliance** across policy and system boundaries
  - Supports **all stakeholders**

http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html



Data Subject

Regulator

Data Protection Officer

Business Owner

Privacy Engineer-Generalist

Privacy Engineer Specialist

Software Engineer

Risk Officer Auditor

Stakeholders

GDPR Principles/ Mandates

Use Case

High Level Analysis

Detailed Analysis

Control Requirements

Services and Functionality

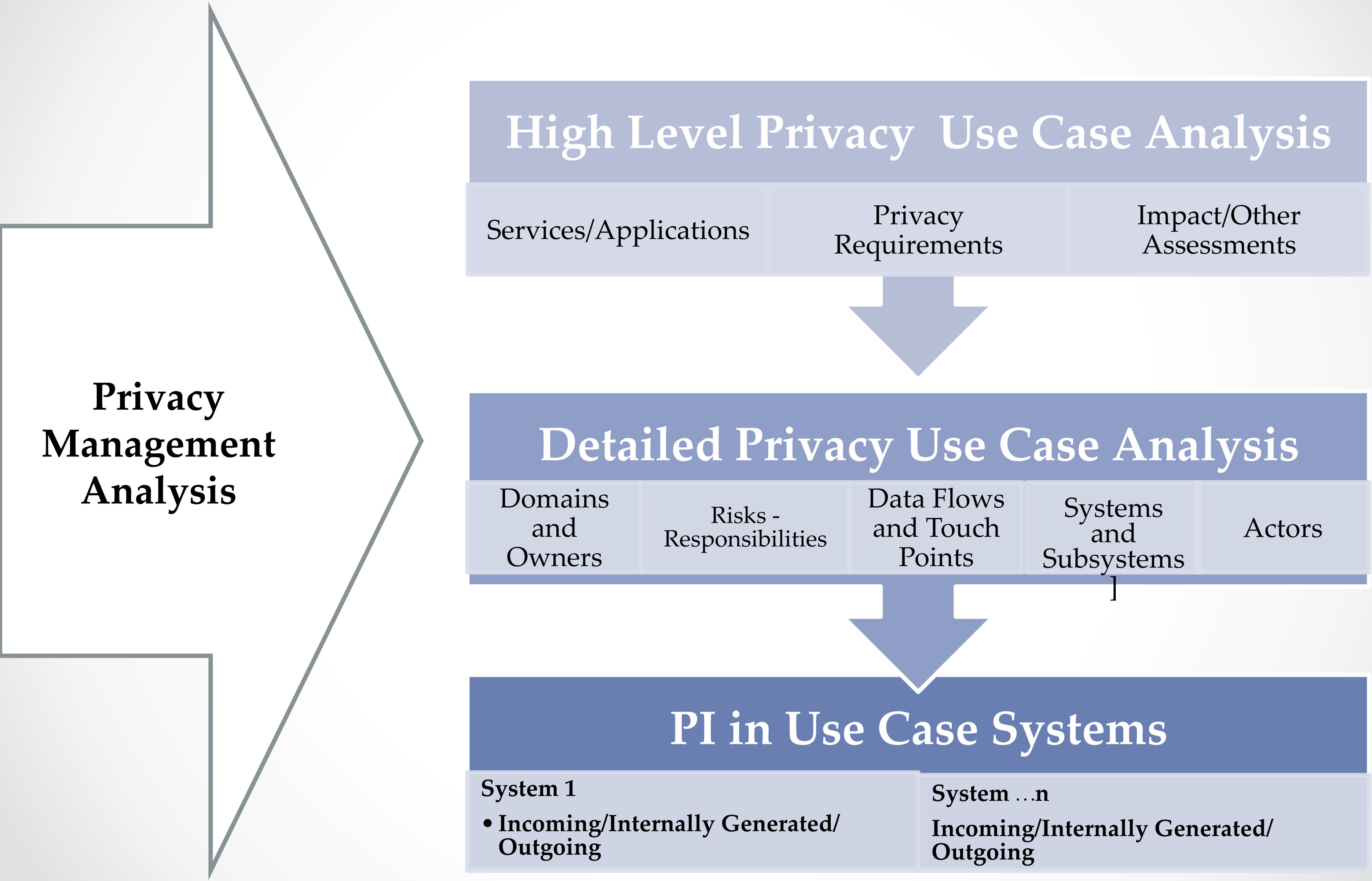
Implementing Mechanisms/ Code

Iterative Risk Analysis

Privacy Management Analysis is complicated

- **Multiple Stakeholders**
- **and Roles**
- **Policies, Procedures**
- **Technical Implementation**
- **Risk Management**
- **SDLC Management**
- **Iterative risk analysis**

PMRM Methodology



Privacy Management Analysis

High Level Privacy Use Case Analysis

Services/Applications

Privacy Requirements

Impact/Other Assessments

Detailed Privacy Use Case Analysis

Domains and Owners

Risks - Responsibilities

Data Flows and Touch Points

Systems and Subsystems
]

Actors

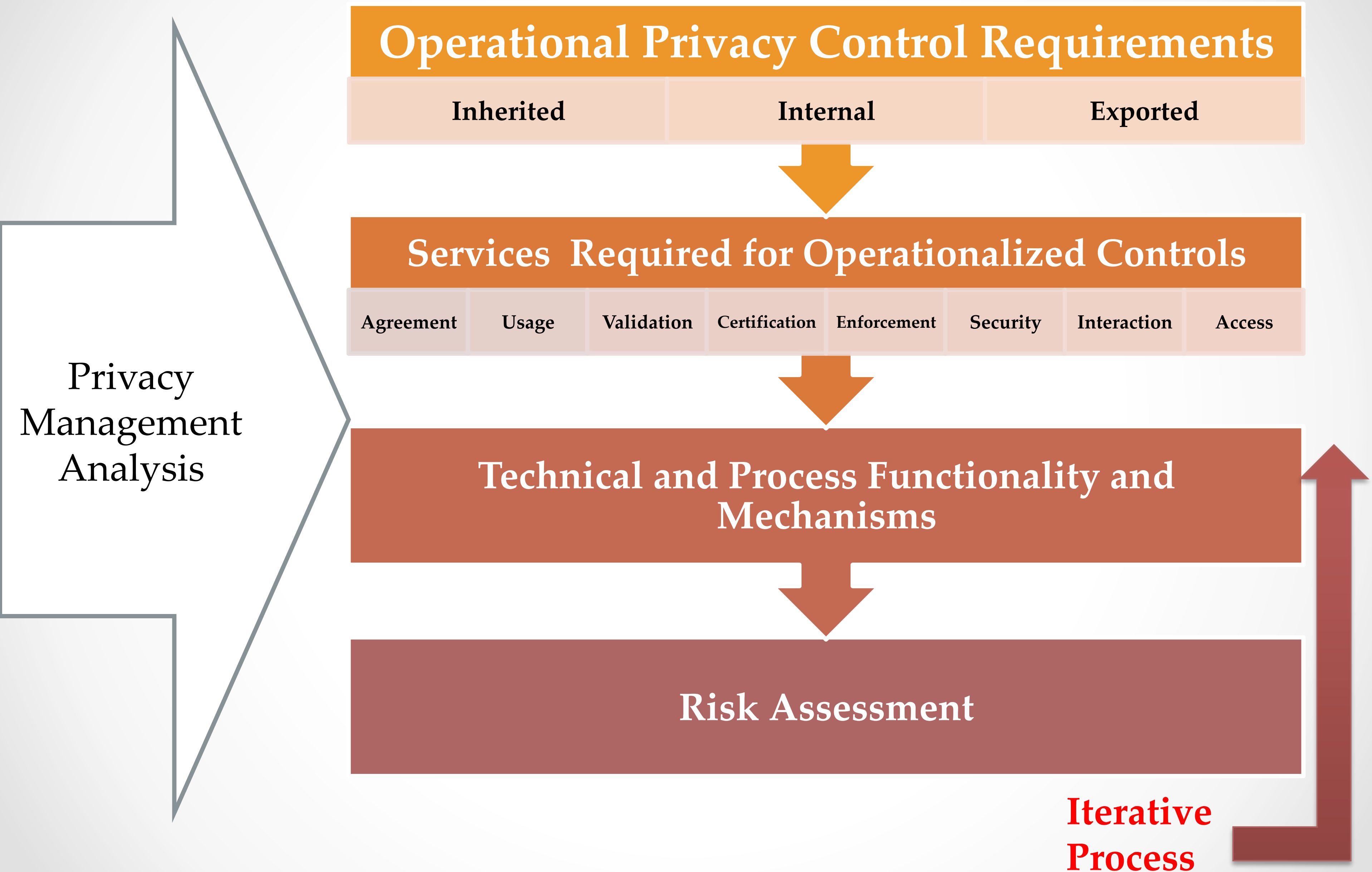
PI in Use Case Systems

System 1

- **Incoming/Internally Generated/ Outgoing**

System …n

Incoming/Internally Generated/ Outgoing



Privacy Management Analysis

Operational Privacy Control Requirements

Inherited | Internal | Exported

Services Required for Operationalized Controls

Agreement | Usage | Validation | Certification | Enforcement | Security | Interaction | Access

Technical and Process Functionality and Mechanisms

Risk Assessment

Iterative Process

Key Actions for GDPR Compliance

Mike Small, Senior Analyst

kuppingercole
ANALYSTS

GDPR – Key Actions

Discovery

Discover and document all the PII you hold.

- Check that it is necessary and minimum.
- Check it is correct and up to date.
- Models for consent and control

Control

Access Control at data field level

- Control of aggregation
- Data Subject access requests
- "Right to be forgotten" and return of data
- Proof that data only used for consented purposes

Consent

Processes for freely given, informed, unambiguous, clear statements of

affirmative actions

- Per purpose and may be revoked at any point of time

GDPR – Key Actions

Cloud

Assure Compliance when data held in cloud services.

- Control over PII in cloud
- Certification of Cloud Service Providers

Data Protection

Data Protection Officers are required

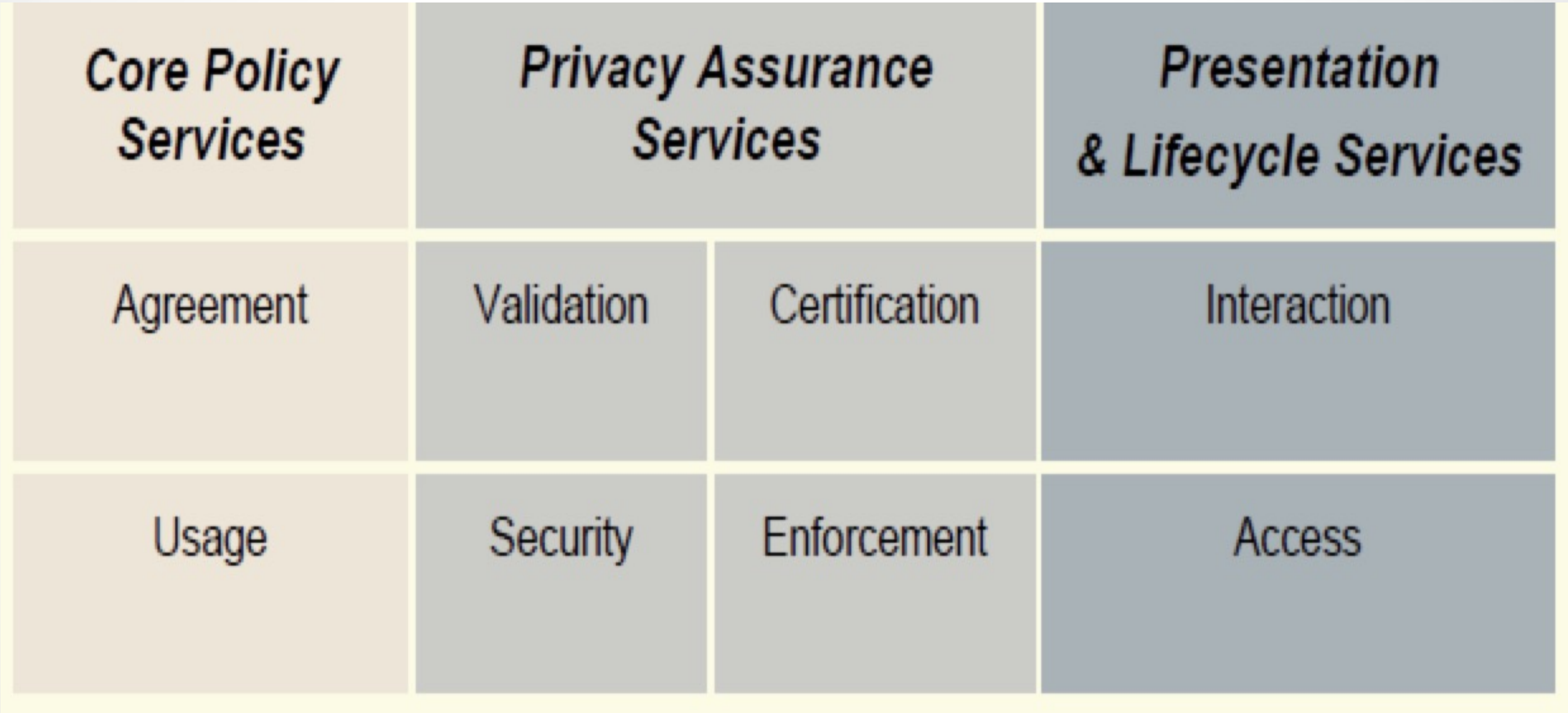
- DPIAs (Data Protection Impact Assessment) under certain circumstances
- Privacy by default and design

Data Breach

Make sure you have the right procedures to detect, report and investigate a breach.

- Communicate to data subjects in clear and plain language.

PMRM *Services*



Core Policy Services	*Privacy Assurance Services*		*Presentation & Lifecycle Services*
Agreement	Validation	Certification	Interaction
Usage	Security	Enforcement	Access

Additional Resources

OASIS PMRM Technical Committee

https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm

Privacy Engineering – GDPR OASIS Workshop Presentation Slides and PMRM Technical Committee Documents

https://www.oasis-open.org/committees/documents.php?wg_abbrev=pmrm&show_descriptions=yes

OASIS Privacy Management Reference Model and Methodology (PMRM)

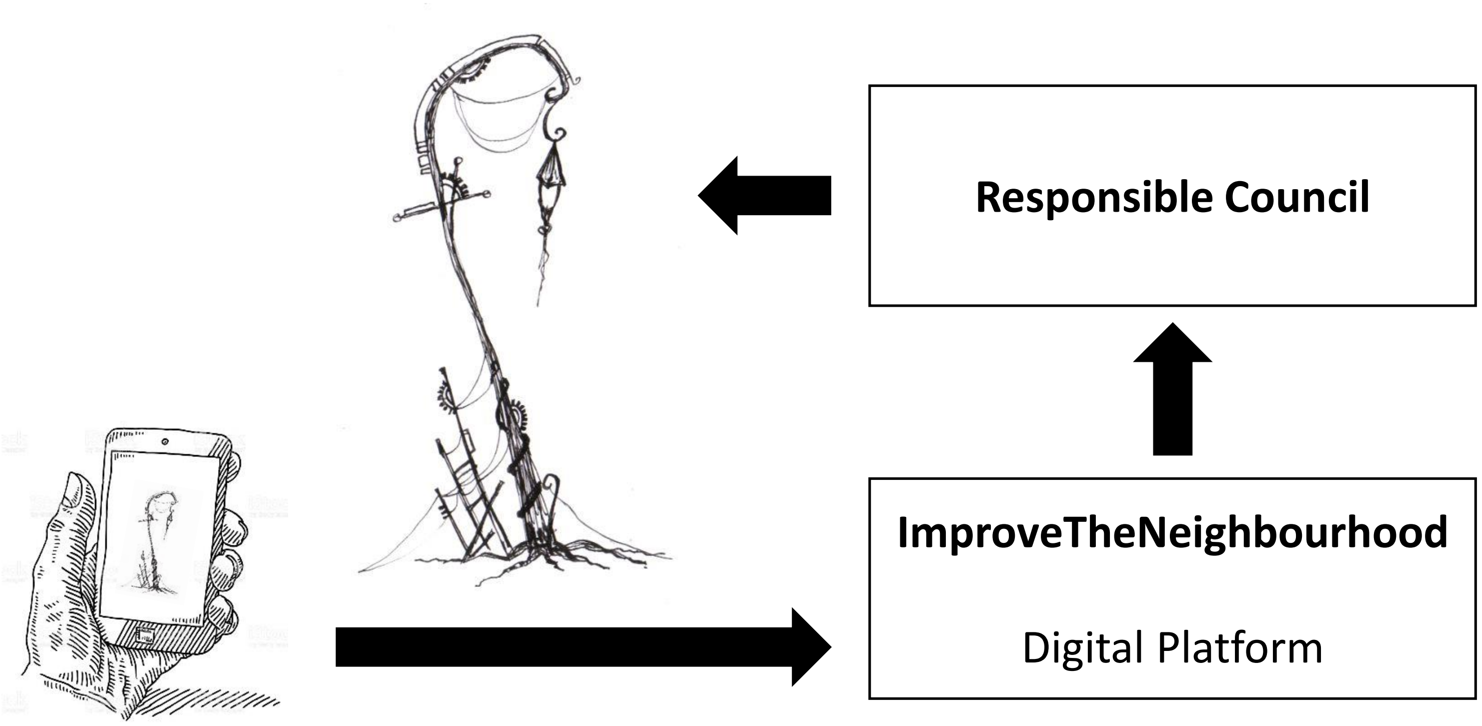
https://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.pdf

OASIS Privacy by Design Documentation for Software Engineers (PbD—SE)

http://docs.oasis-open.org/pbd-se/pbd-se/v1.0/csd01/pbd-se-v1.0-csd01.pdf

Overview of Use Case

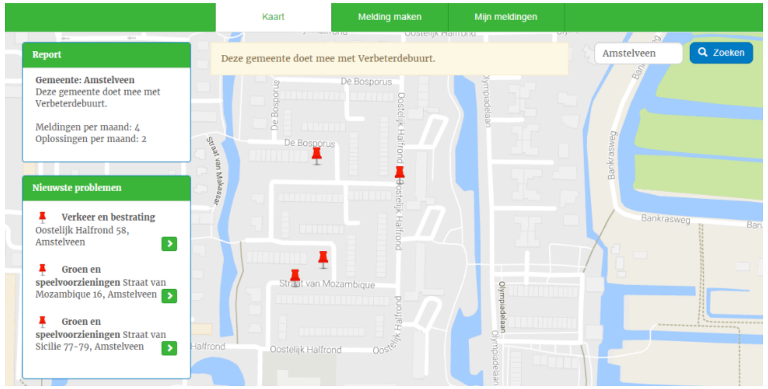
- Use Case: ImproveTheNeighbourhood



Responsible Council

ImproveTheNeighbourhood

Digital Platform



Report

Gemeente: Amstelveen
Deze gemeente doet mee met Verbeterdebuurt.

Meldingen per maand: 4
Oplossingen per maand: 2

Deze gemeente doet mee met Verbeterdebuurt.

Nieuwste problemen

Verkeer en bestrating Oostelijk Halfrond 58, Amstelveen

Groen en speelvoorzieningen Straat van Mozambique 16, Amstelveen

Groen en speelvoorzieningen Straat van Sicilie 77-79, Amstelveen

PMRM PMA Analysis

PMRM tasks 1 to 18

- Task #1 - Use Case Description
- Task #2 - Use Case Inventory
- Task #3 - Privacy Policy Conformance Criteria
- Task #4 - Assessment Preparation
- Task #5 - Identify Participants
- Task #6 - Identify Systems and Business Processes
- Task #7 - Identify Domains and Owners
- Task #8 - Identify Roles and Responsibilities within a Domain
- Task #9 - Identify Touch Points
- Task #10 - Identify Data Flows
- Task #11 - Identify Incoming PI
- Task #12 - Identify Internally Generated PI
- Task #13 - Identify Outgoing PI
- Task #14 - Specify Inherited Privacy Controls
- Task #15 - Specify Internal Privacy Controls
- Task #16 - Specify Exported Privacy Controls
- Task #17 - Identify the Services and Functions necessary to support operation of identified Privacy Controls
- Task #18 - Identify the Mechanisms that Implement the Identified Services and Functions

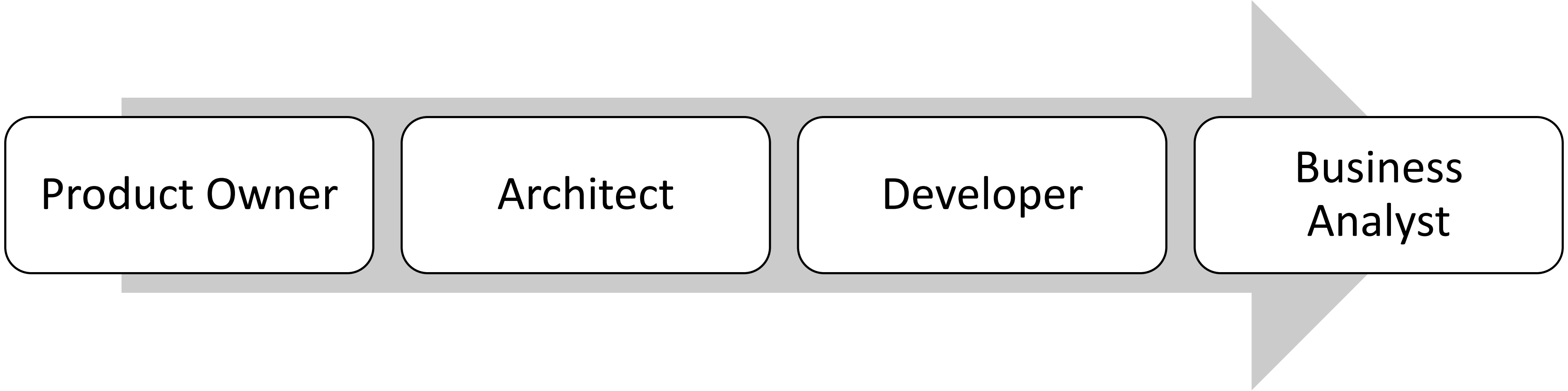
PMRM PMA Analysis

“Responsibilities” Table

Stake-holders/Lead	Use Case Description	Systems	Participants	PI/PII	Domains	Legal/Regs/ Policies	Data Flows/Touch points	Systems	Privacy Controls	Services - Technical Functions
CPO	x		x	x	x	x			x	
IT Architect					x		x		x	x
Business Analyst	x	x	x		x		x			
Team Privacy Champion			x	x		x	x		x	
Senior Developer		x						x	x	x
Line of Business Owner	x	x			x				x	
Legal Department					x	x				x
CIO						x		x		x
Data Center Director					x			x		x

PMRM PMA Analysis

Iterative steps with stakeholders



Task #5 - Identify Participants

- Citizen
- Fieldworker

Task #6 - Identify Systems

- VBDB Web App
- VBDB Fieldworker App

Task #7 - Identify Domains

- Citizen
- VBDB Platform
- Councils

Task #9 - Identify Touch Points

- VBDB Mobile App - VBDB System
- VBDB Fieldworker App - VBDB System

Task #10 - Identify Data Flows

Task #11 - Identify Incoming PI

Task #12 - Internally Gen. PI

Task #13 - Identify Outgoing PI

- Picture
- Email address

PMA Interview with Product Owner

Task #5 - Identify Participants

- Citizen
- Fieldworker
- Backoffice Employee
- Customer Support Employee

Task #6 - Identify Systems

- VBDB Web App
- VBDB Fieldworker App
- VBDB Web App
- VBDB Mail
- VBDB System
- CRMOnline
- Case Management System

Task #7 - Identify Domains

- Citizen
- VBDB Platform
- Councils:
    - Council Type 1
    - Council Type 2
    - Council Type 3
    - Council Type 4

Task #9 - Identify Touch Points

- VBDB Mobile App - VBDB System
- VBDB Fieldworker App - VBDB System
- VBDB Web App - VBDB System
- VBDB System - Case Management System
- VBDB System - CRMOnline
- VBDB System - Mail system

Task #10 - Identify Data Flows

- Citizen - VBDB Platform
- Council Type 2 - VBDB Platform

Task #11 - Identify Incoming PI

Task #12 - Internally Gen. PI

- Personalized interests

Task #13 - Identify Outgoing PI

- Picture
- Email address

PMA Interview with Architect

Task #5 - Identify Participants

- Citizen
- Fieldworker
- Backoffice Employee
- Customer Support Employee

Task #6 - Identify Systems

- VBDB Web App
- VBDB Fieldworker App
- VBDB Web App
- VBDB Mail
- VBDB System
- CRMOnline
- Case Management System
- MailChimp
- ActiveMQ
- Mule
- Postfix
- Postmark
- ArgisOnline
- ArgisPro

Task #7 - Identify Domains

- Citizen
- VBDB Platform
- Councils:
  - Council Type 1
  - Council Type 2
  - Council Type 3
  - Council Type 4
- Rocket Science Group
- ESRI
- Wildbit
- LeaseWeb
- OVH

Task #9 - Identify Touch Points

- VBDB Mobile App - VBDB System
- VBDB Fieldworker App - VBDB System
- VBDB Web App - VBDB System
- VBDB System - Case Management System
- VBDB System - CRMOnline
- VBDB System - Mail system

Task #10 - Identify Data Flows

- Citizen - VBDB Platform
- Council Type 2 - VBDB Platform

Task #11 - Identify Incoming PI

Task #12 - Internally Gen. PI

- Personalized interests

Task #13 - Identify Outgoing PI

- Picture
- Email address

PMA Interview with Developer

Task #5 - Identify Participants

- Citizen
- Fieldworker
- Backoffice Employee
- Customer Support Employee

Task #6 - Identify Systems

- VBDB Web App
- VBDB Fieldworker App
- VBDB Web App
- VBDB Mail
- VBDB System
- CRMOnline
- Case Management System
- MailChimp
- ActiveMQ
- Mule
- Postfix
- Postmark
- ArgisOnline
- ArgisPro
- Melddesk
- DMS
- GBA
- Workflow Engine
- Personal Internet Page

Task #7 - Identify Domains

- Citizen
- VBDB Platform
- Councils:
  - Council Type 1
  - Council Type 2
  - Council Type 3
  - Council Type 4
- Rocket Science Group
- ESRI
- Wildbit
- LeaseWeb
- OVH

Task #9 - Identify Touch Points

- VBDB Mobile App - VBDB System
- VBDB Fieldworker App - VBDB System
- VBDB Web App - VBDB System
- VBDB System - Case Management System
- VBDB System - CRMOnline
- VBDB System - Mail system

Task #10 - Identify Data Flows

- Citizen - VBDB Platform
- Council Type 2 - VBDB Platform

Task #11 - Identify Incoming PI

Task #12 - Internally Gen. PI

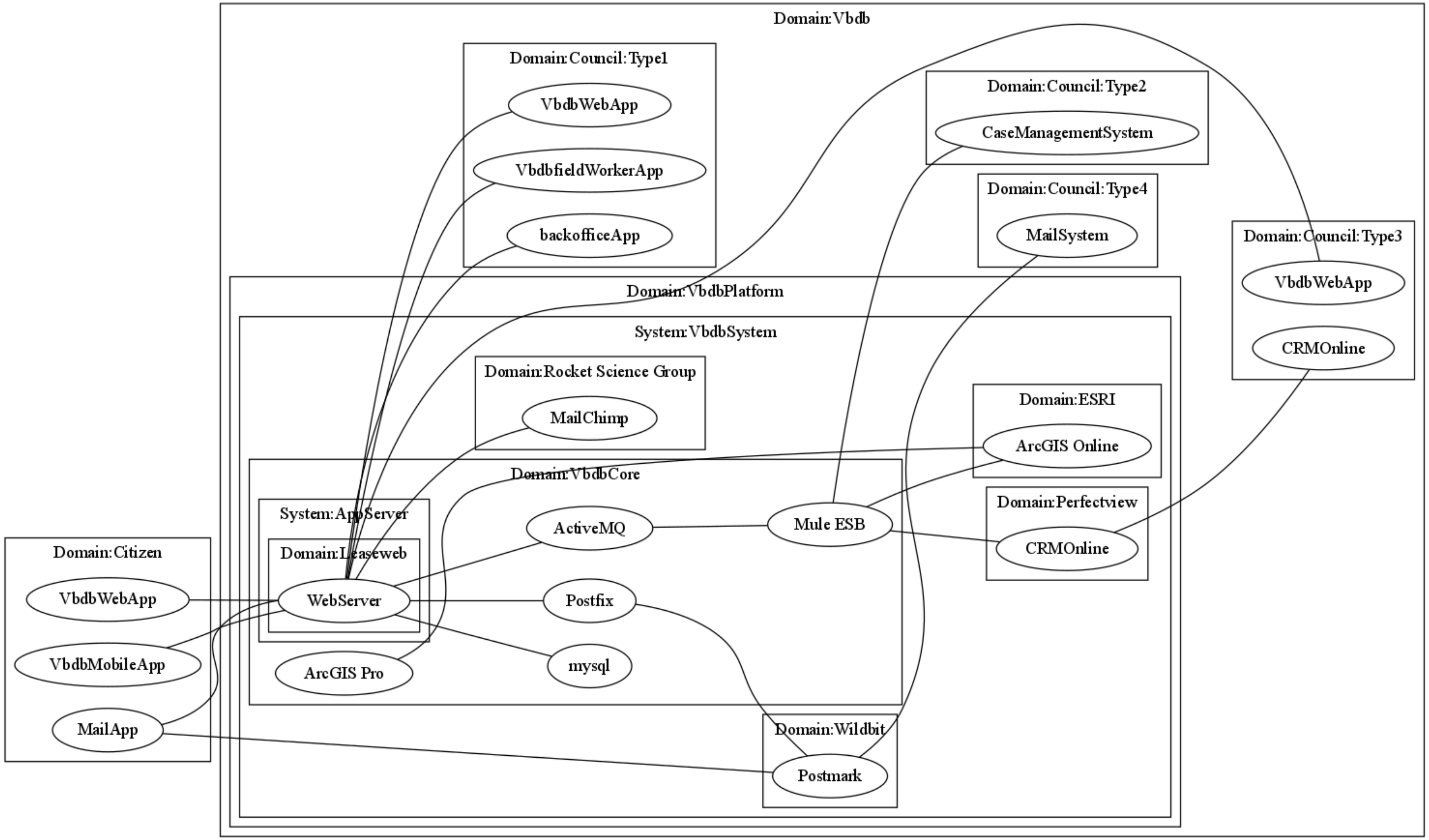
- Personalized interests

Task #13 - Identify Outgoing PI

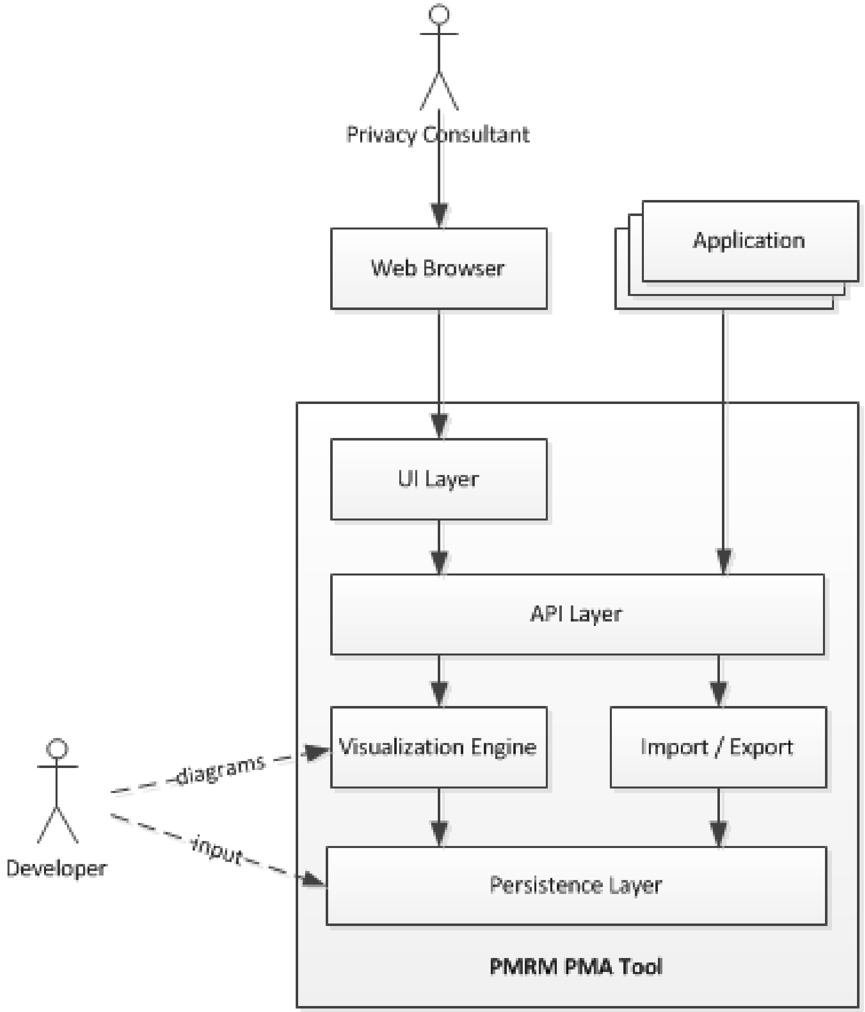
- Picture
- Email address
- First name
- Last name
- Gender
- Home Address
- Phone number
- Screen name
- Time
- Date
- Geo-tag information
- Picture metadata
- IP address
- Connection specific data: device type, browser, toolkit,etc.

PMA Interview with Business Analyst

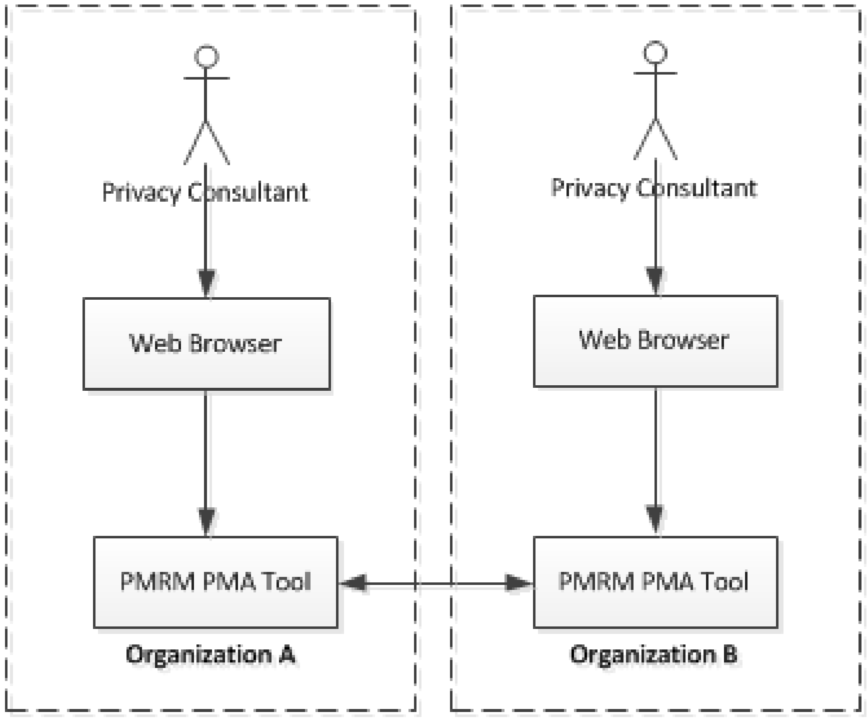
PMRM PMA Analysis - Diagram



Architecture of PMRM PMA tool



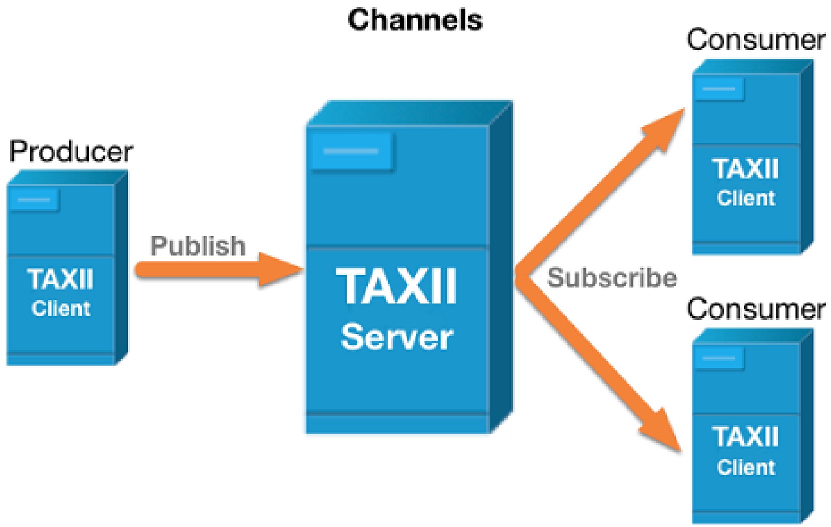
Architecture of PMRM PMA tool

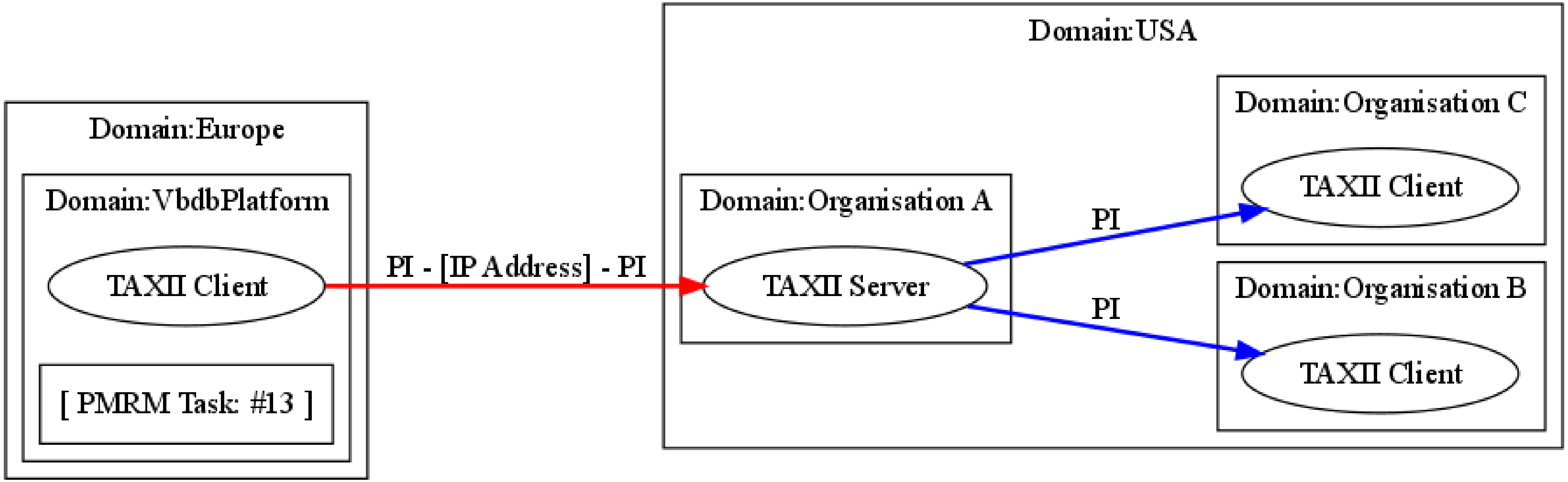


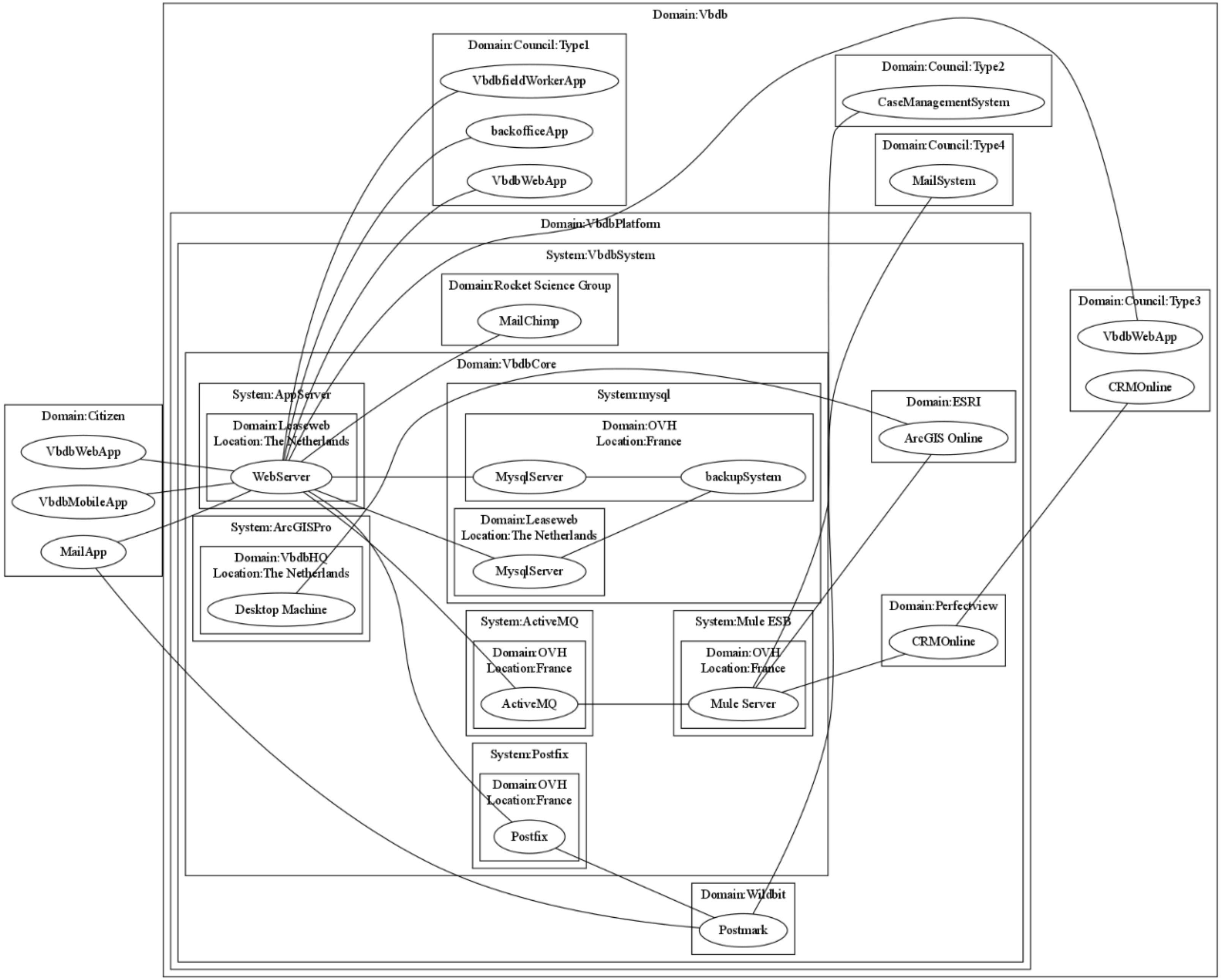
Small example: outgoing PI

- Thinking about the CTI infrastructure & GDPR
  - Using the visual representations
  - Outgoing PI example in shared thread information

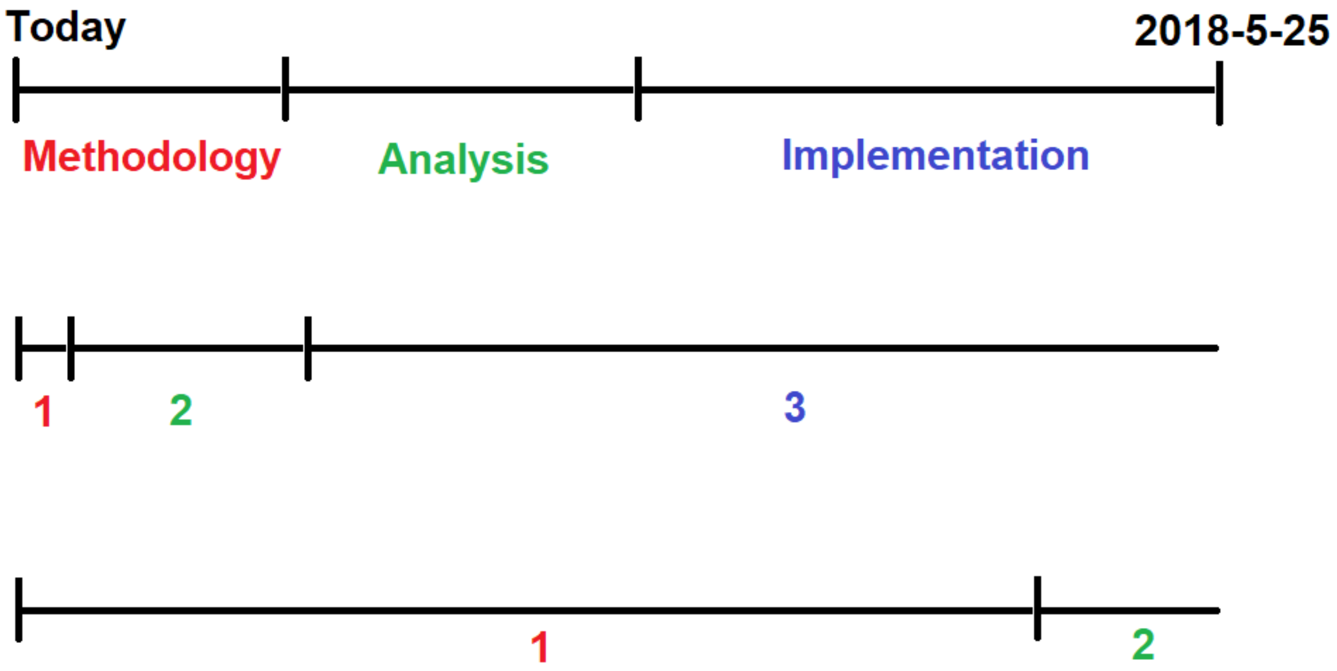
Basic TAXII setup




Domain:Europe
Domain:VbdbPlatform
TAXII Client
[PMRM Task: #13]
PI - [IP Address] - PI
Domain:USA
Domain:Organisation A
TAXII Server
PI
PI
Domain:Organisation C
TAXII Client
Domain:Organisation B
TAXII Client


Domain:Vbdb
Domain:Council:Type1
VbdbfieldWorkerApp
backofficeApp
VbdbWebApp
Domain:Council:Type2
CaseManagementSystem
Domain:Council:Type4
MailSystem
Domain:VbdbPlatform
System:VbdbSystem
Domain:Rocket Science Group
MailChimp
Domain:Council:Type3
VbdbWebApp
CRMOnline
Domain:VbdbCore
System:AppServer
Domain:Leaseweb
Location:The Netherlands
WebServer
System:mysql
Domain:OVH
Location:France
MysqlServer
backupSystem
Domain:ESRI
ArcGIS Online
Domain:Citizen
VbdbWebApp
VbdbMobileApp
MailApp
System:ArcGISPro
Domain:VbdbHQ
Location:The Netherlands
Desktop Machine
Domain:Leaseweb
Location:The Netherlands
MysqlServer
Domain:Perfectview
CRMOnline
System:ActiveMQ
Domain:OVH
Location:France
ActiveMQ
System:Mule ESB
Domain:OVH
Location:France
Mule Server
System:Postfix
Domain:OVH
Location:France
Postfix
Domain:Wildbit
Postmark

Value of tool


Today
2018-5-25
Methodology
Analysis
Implementation
1
2
3
1
2