OASIS IDtrust

PMRM Overview and Privacy Management Analysis Tools Development

John Sabo
John.annapolis@verizon.net
Gershon Janssen
gershon.janssen@gmail.com @gershonjanssen

"Smart" and Privacy

- **Smart Grid:** "A **smart grid** is a modernized electrical grid that uses **analog or digital information and communications technology to gather and act on information,** such as information about the **behavior of suppliers and consumers** , in an automated fashion, to improve the efficiency, reliability, economics and sustainability of the production and distribution of electricity."

- **Smart City: "**A city can be defined as 'smart' when investments in human and social capital and traditional (transport) and **modern (ICT) communication infrastructure** fuel sustainable economic development and a high quality of life…through **participatory action and engagement…..** Online collaborative sensor data management platforms are on-line database services that allow sensor owners to **register and connect their devices to feed data into an online database for storage and also allow developers to connect to the database and build their own applications based on that data.**

- **Smart Phone: "**A **smart phone** … is a mobile phone with more advanced computing capability **and connectivity** than basic feature phones."

- **Internet of Things: "**The Internet of Things (IoT) refers to **uniquely identifiable objects** and their virtual representations in an Internet-like structure. Today …IoT… is used to denote **advanced connectivity of devices, systems and services** and covers a **variety of protocols, domains and applications**."

(Definitions: Wikipedia)

Smart: Connectivity, Information and Context

- "Your phone is constantly gathering what app developers call signals. These could be your commuting habits, which the phone can glean from its internal GPS, often within a few feet. Your phone could also gather your meetings, your future trips, your friends and family, your favorite sports team, the type of news you usually read and even things like your heart rate. Things really get interesting when the apps that gather these signals start to be predictive. When that happens, your phone can start anticipating your needs, interests and habits …." ***Examples:*** Google Now, Cortana, EverythingMe, Mynd, EasilyDo…."

- "Contextual is a whole world," said Ami Ben David, co-founder of the company EverythingMe. "We're going to start looking at computers as being smart, as having infinite computing power and infinite access to databases, and therefore able to talk to us and give us what we want."

(Molly Wood, *New York Times*, May 7, 2014: http://www.nytimes.com/2014/05/08/technology/personaltech/the-app-that-knows-you.html?emc=eta1

Smart: How do We Design in Privacy?

Understanding "Smart" Applications and *Designing in* Privacy

- Gaps
  - Discontinuity between policies and technology
  - Speed to market – innovation
  - Complexity and scale
  - Lack of standards
  - Privacy Focus: macro or micro?

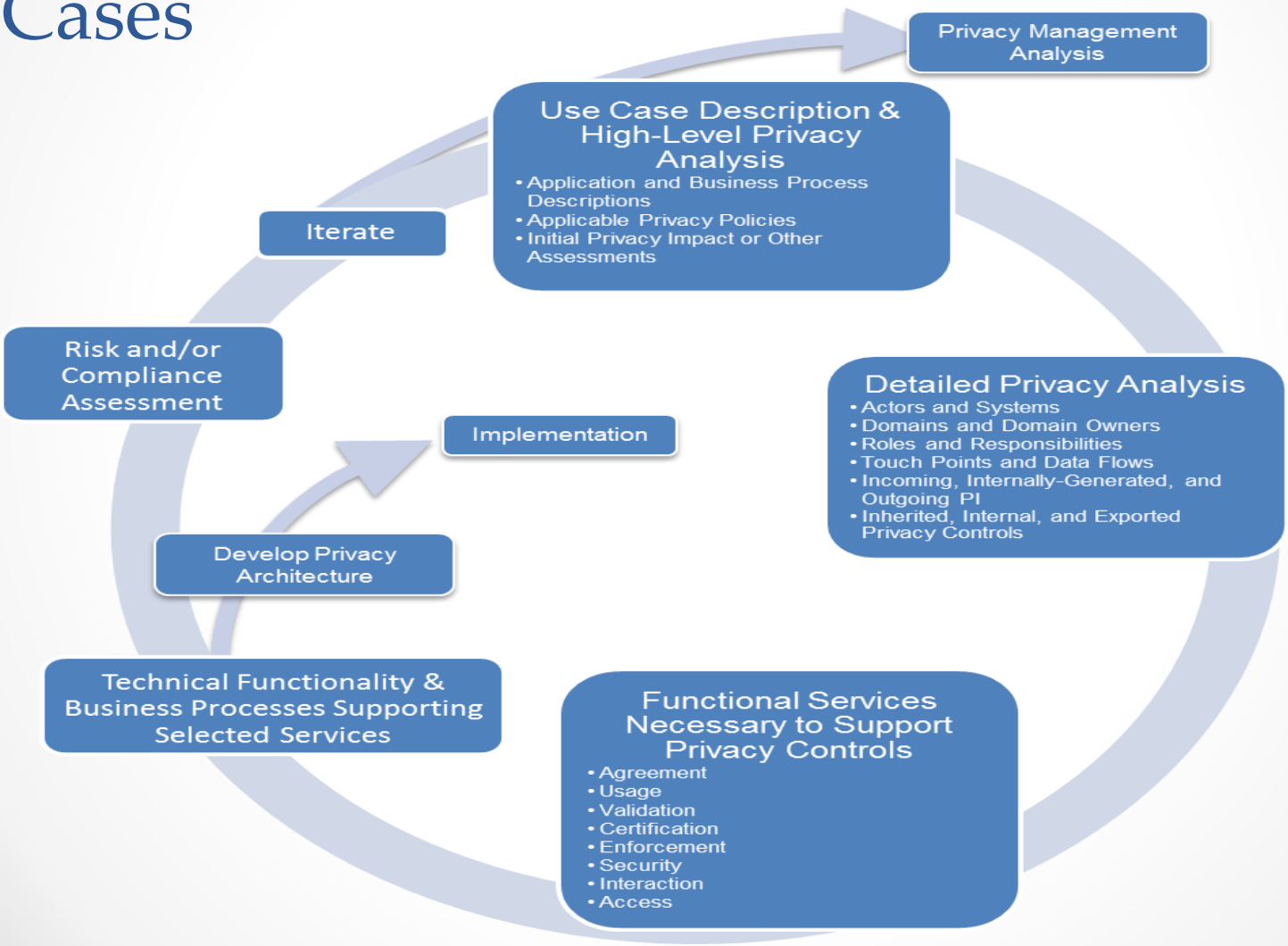
- Work Underway in OASIS
  - OASIS PBD-SE Technical Specification (under development)
  - OASIS PMRM Committee Specification v1.0 and use case work
  - XACML Profiles

- Emerging Tools
  - "Privacy by Design Use Case Template"
    - Derived from PMRM and PbD technical committee collaboration

Privacy Use Case Template as Tool Supporting Privacy by Design

- Provides all stakeholders associated with the specified software development project within an organization a common picture and a clearer understanding of *all* relevant privacy components of the project
- Can expose gaps where PbD analysis has not been carried out where implementation has not been initiated or completed
- A tool to map privacy policies, requirements and control objectives to technical functionality
- Facilitates the re-use of knowledge for new applications and the extension of Privacy by Design principles more broadly throughout an organization
- Where code must bridge to external systems and applications, a standardized template will help ensure that Privacy by Design principles extend to the transfer of personal information across system and organizational boundaries.
- A standards-based use case template can reduce the time and cost of operationalizing PbD and improve the quality and reusability of documentation

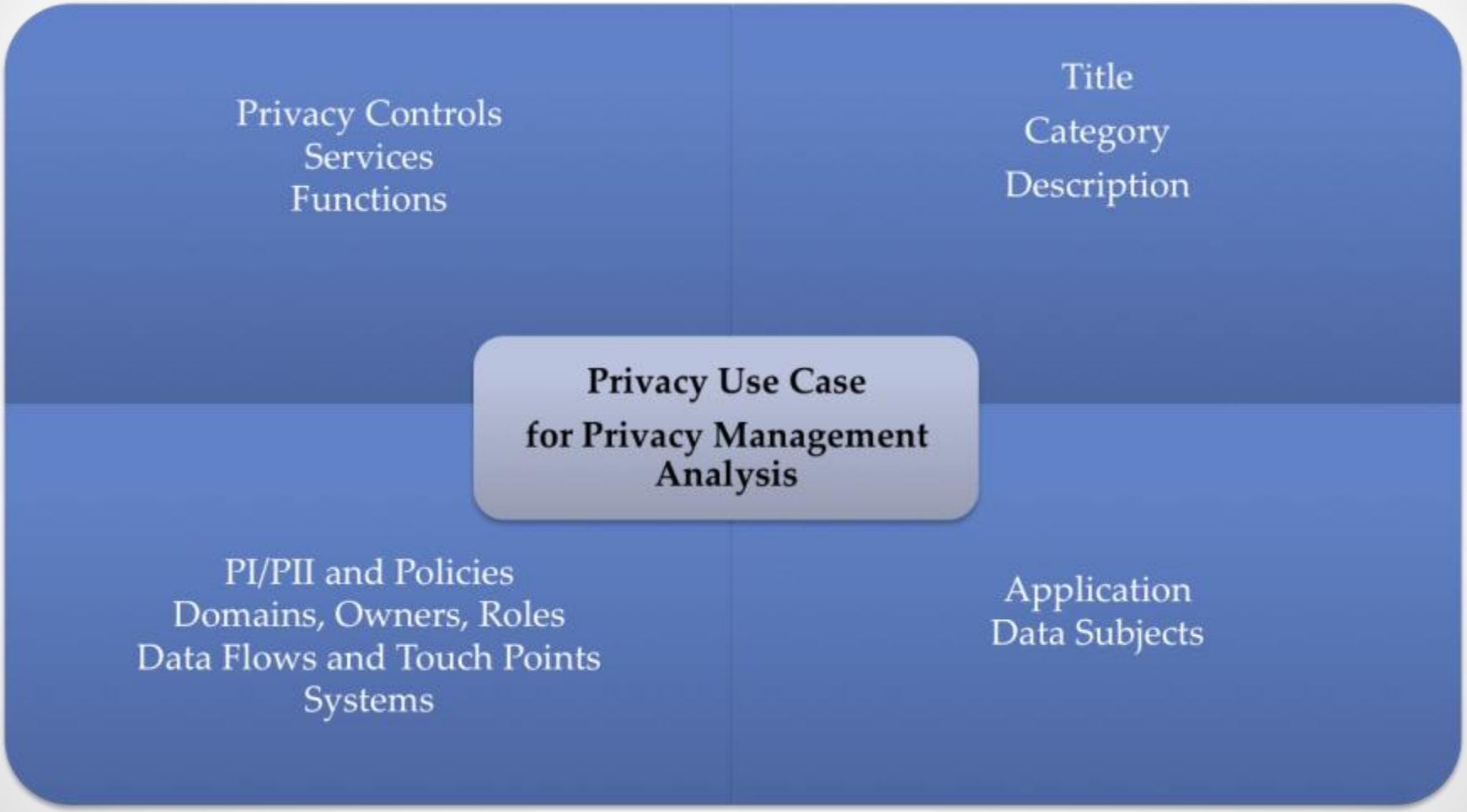
PMRM v1.0 Methodology Designed to Make Possible Analysis of Complex Use Cases



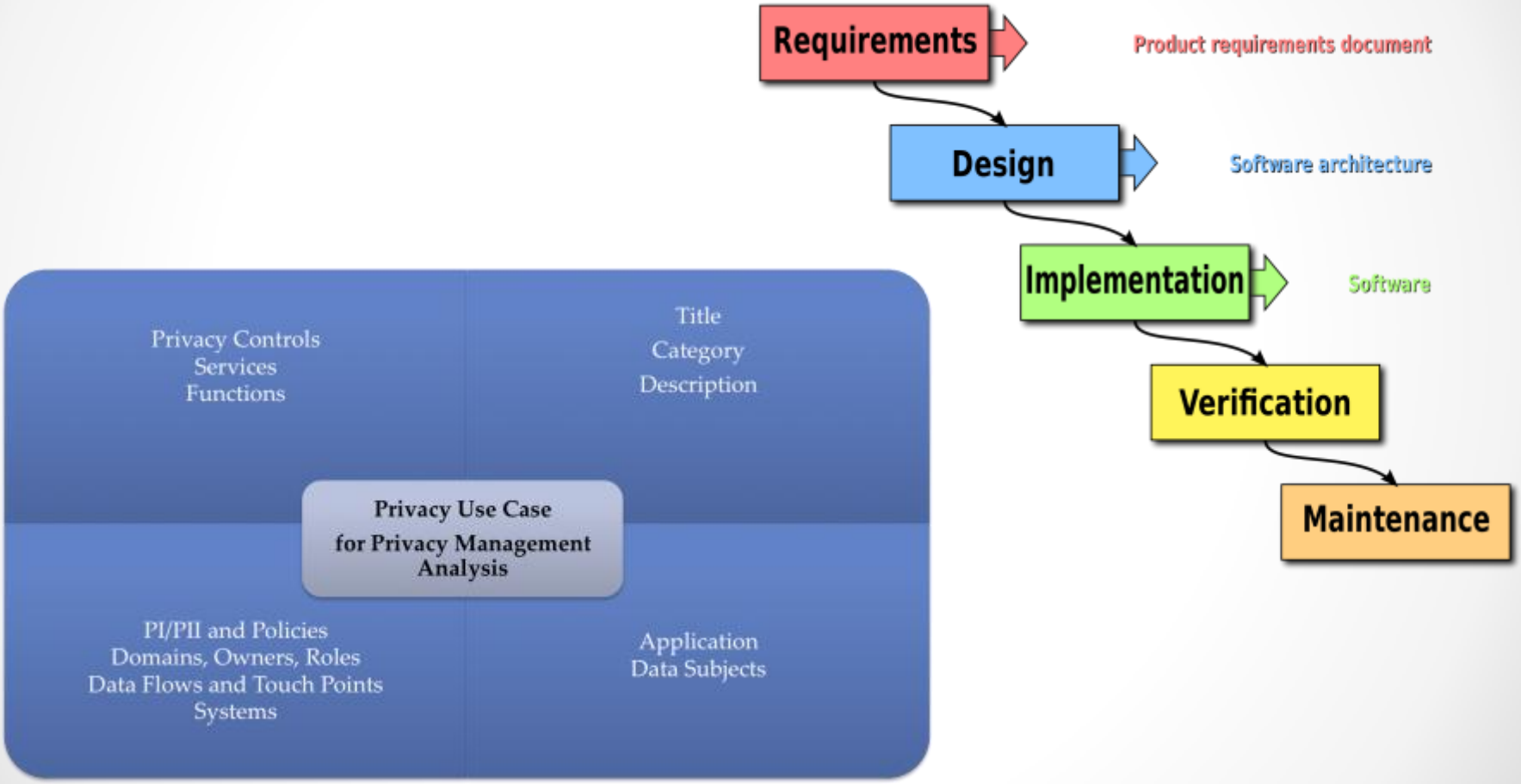
PMRM-Based Template Benefits

- Provides an inventory of Privacy Use Case components and the responsible parties that directly affect software development for the Use Case
- Segments Privacy Use Case components in a manner generally consistent with the OASIS PMRM v1.0 Committee Specification
- Enables understanding of the relationship of the privacy responsibilities of software developers vis-à-vis other relevant Privacy Use Case stakeholders
- Bring insights to the privacy aspect when moving through the different stages of the privacy lifecycle and across interconnected applications
- May be extended to address predicates for software developers (training, privacy management maturity, etc.)
- Does not specify an implementer's SDLC methodology, development practices or in-house data collection, data analysis or modeling tools
- Valuable as a tool to increase opportunities to achieve Privacy by Design in applications by extracting and making visible required privacy properties
- Enables Capability Maturity Model analysis for an organization

Privacy Use Case Template

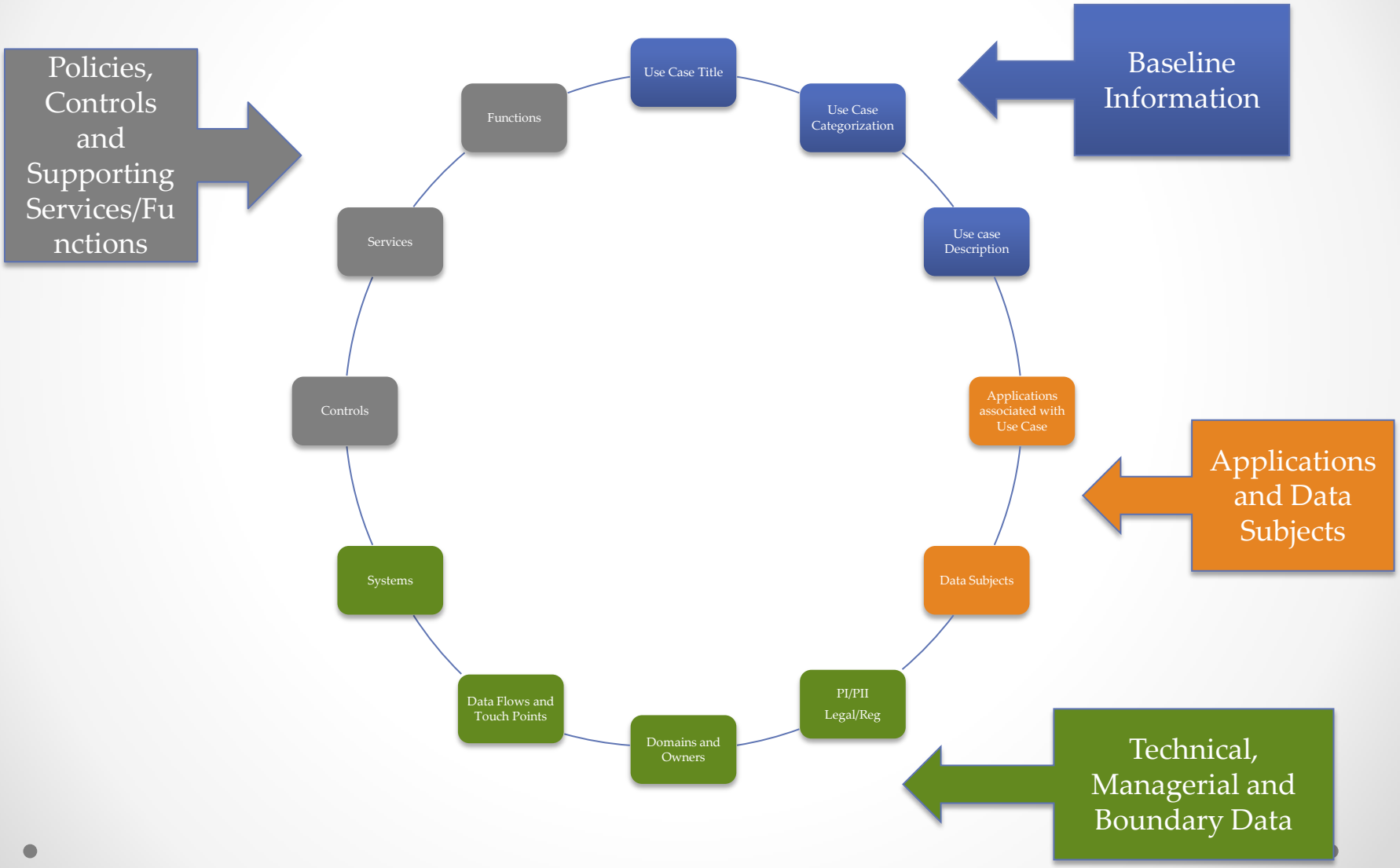


Template Helps Address Challenge of Mapping Privacy Analysis to Software Development Lifecycle Processes



SDLC Graphic Source: Wikipedia Commons

PMRM Template
Privacy Management Analysis (PMA)



Baseline Information

Use Case Title

A short descriptive title for the use case

ACME Insurance Company Vehical Data Tracking for Reduced Premiums

Baseline Information

Category of Use Case

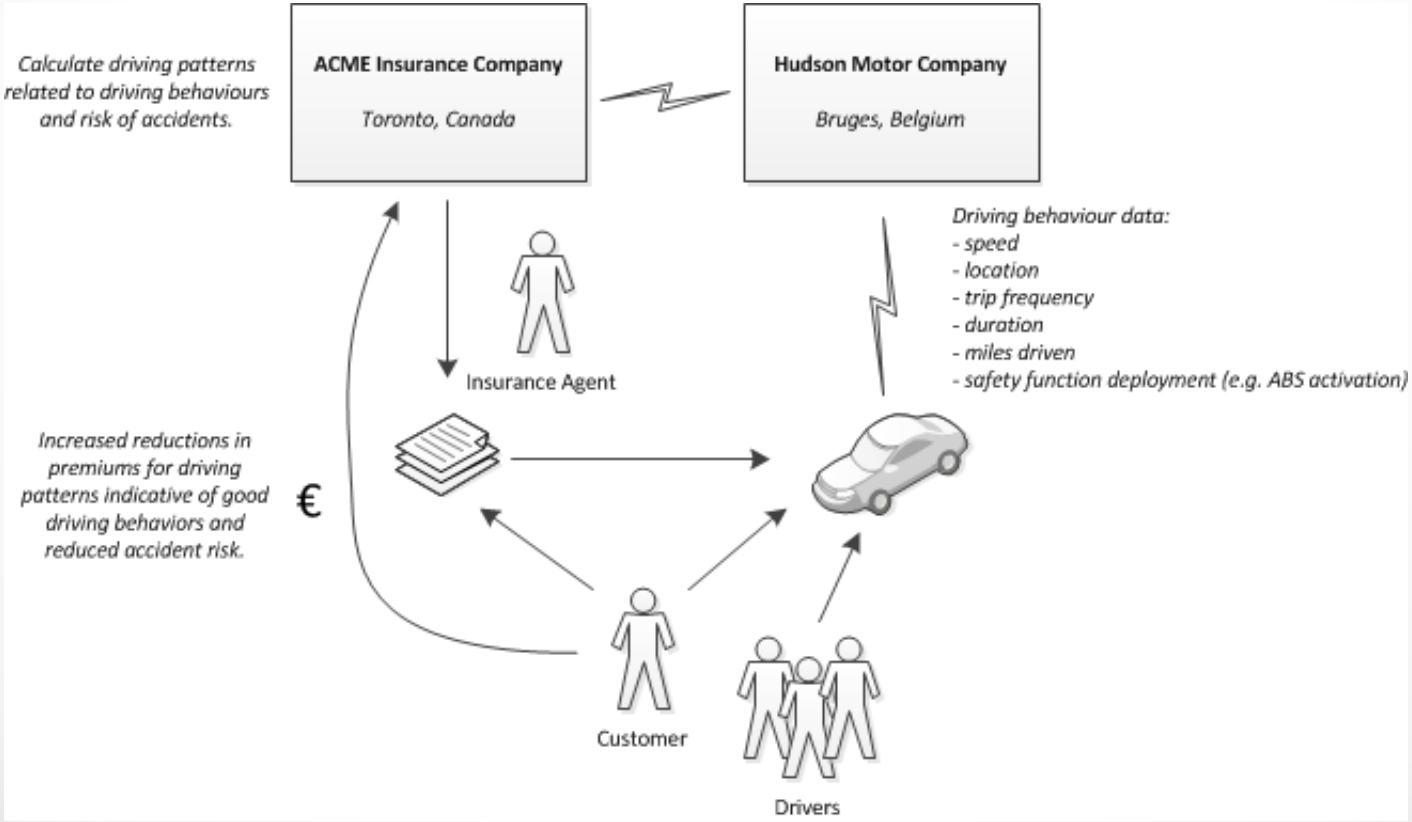
e.g. Application categories such as "Online Banking" or Model categories such as "Two Domain".

Mobile-Vehicular

Baseline Information

↳ Use Case Description

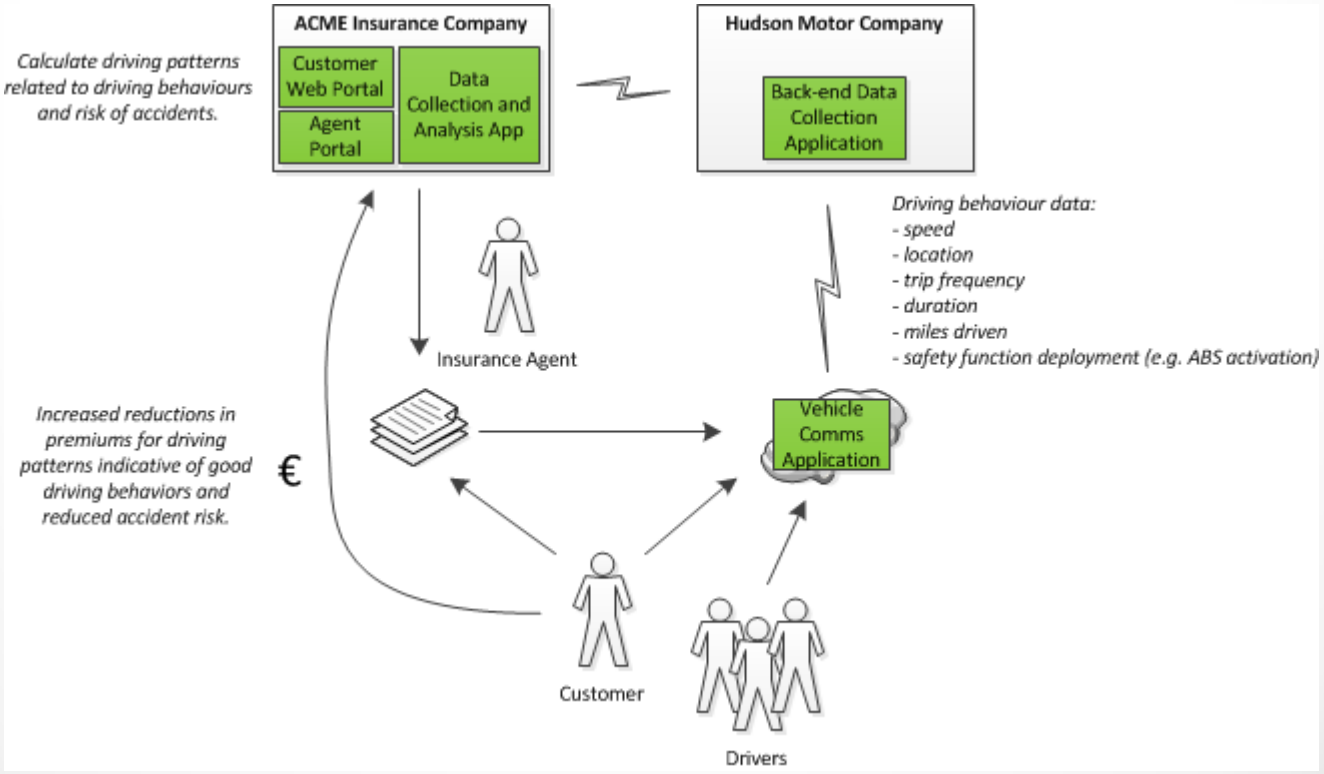
High-level synopsis of the use case.



Applications and Data Subjects

Applications associated with Use Case

Relevant applications and products where personal information is communicated, created, processed, stored or deleted and requiring software development

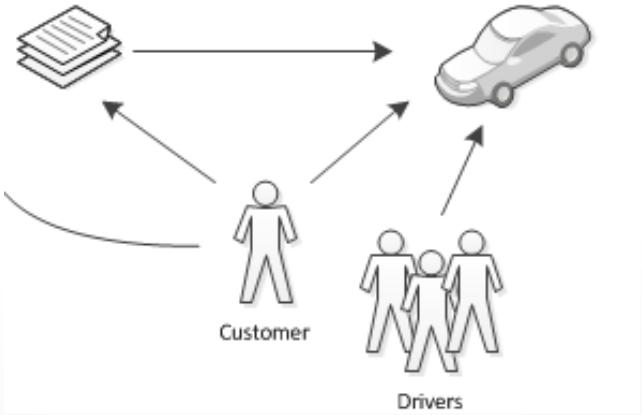


Applications and Data Subjects

↳ Data subject(s) associated with Use Case

Include any data subjects associated with any of the applications in the use case.

- *The registered Insured person associated with the vehicle VIN*
- *Other drivers designated by the vehicle owner*



Technical, Managerial and Boundary Data

↳ PI and PII covered by the Use Case

The PI and PII collected, created, communicated, processed, stored or deleted within privacy domains or systems, applications or products.

- per domain, system, application or product depending on level of use case development
- including incoming, internally generated and outgoing PI

- *Registered driver name, Account Number, VIN*
- *Registered driver contact information*
- *Linked vehicle operational data*
- *Linked vehicle time and location data*
- *Linked evaluation assessment and summary information*

Technical, Managerial and Boundary Data

Legal, regulatory and/or business policies governing PI and PII in the Use Case

The policies and regulatory requirements governing privacy conformance within use case domains or systems and links to their sources.

- *Government(s) regulations*
- *Vehicle Manufacturer privacy policies*
- *Telecom Carrier privacy policies*
- *Insurance Company privacy policies*
- *Data Subject Consent preferences*
- *Specific policies governing apps (e.g., "Data Communications to Manufacturer"*
- *Links to policies ….*
  - *http://acmeinsurancegroupinc.biz/vehicle privacy/*
  - *http://HudsonCarCompany.biz/privacy_vehicle….*

Technical, Managerial and Boundary Data

Domains, Domain Owners, and Roles associated with Use Case

- **Domains** - both physical areas (such as a customer site or home) and logical areas (such as a wide-area network or cloud computing environment) that are subject to the control of a particular domain owner

- **Domain Owners** - the stakeholders responsible for ensuring that privacy controls and functional services are defined or managed in business processes and technical systems within a given domain

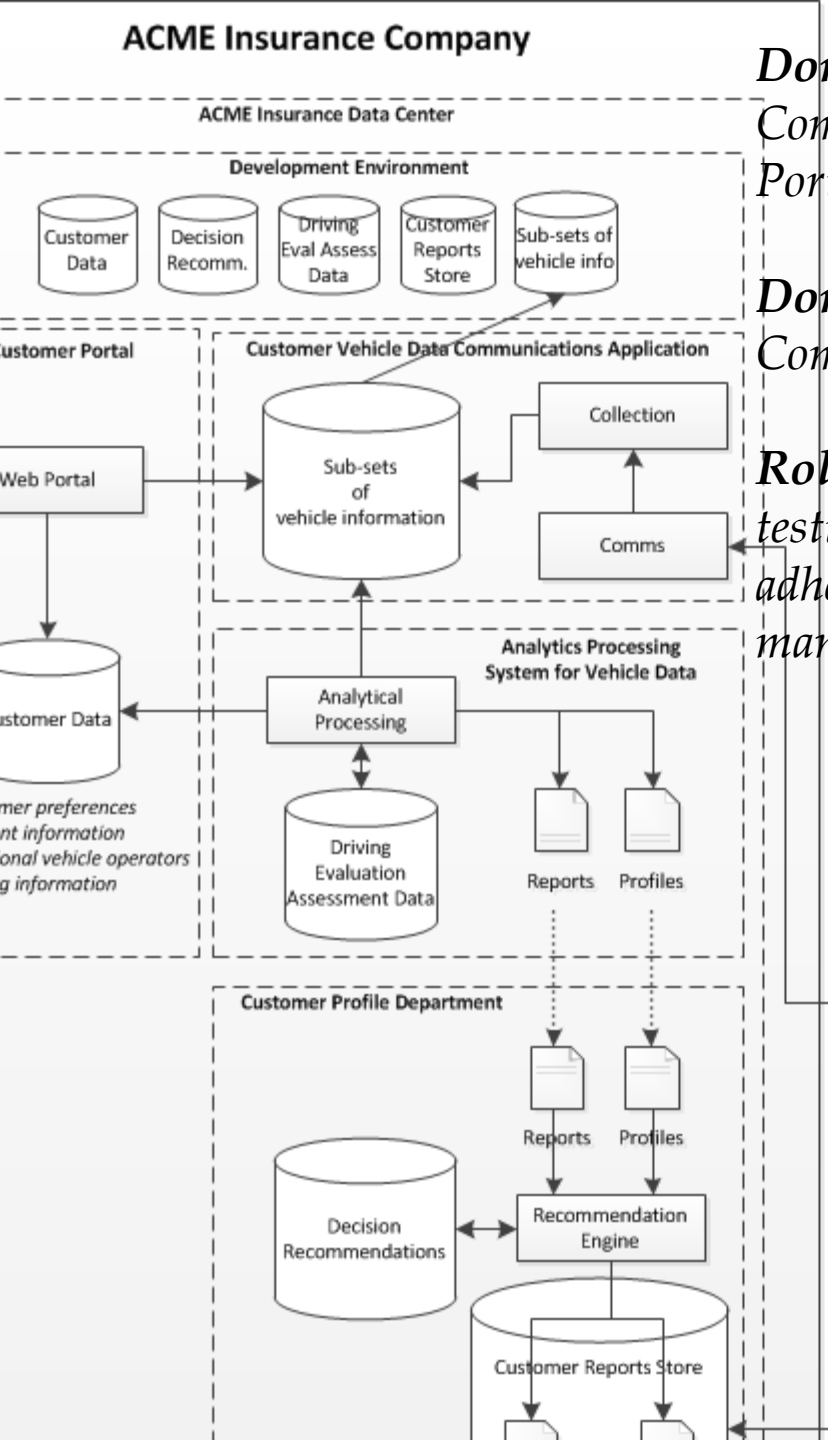
  Note: Identifying stakeholders is essential for clarifying the intersection of privacy requirements and software development.

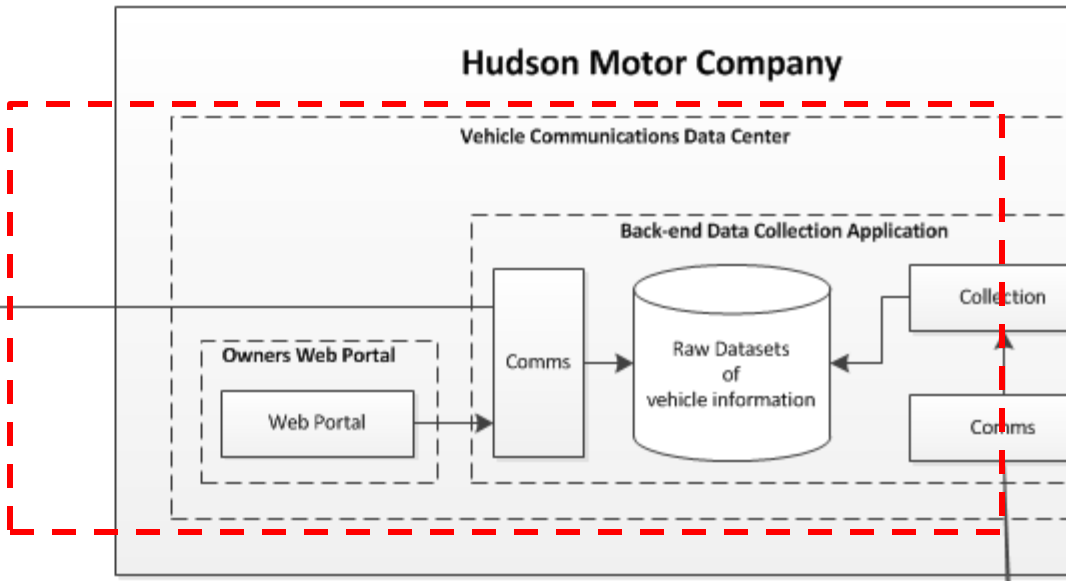
- **Roles** - the roles and responsibilities assigned to specific stakeholders and their relationship to systems within a specific privacy domain

Domain 1: *Hudson Motor Company's Vehicle Communications Data Center, Vehicle Owner's Web Portal and Backend Data Collection Application*

Domain 1 Owner: *VP, Vehicle Manufacturer's Vehicle Communication and Data Division*

Role: *Application design, development, content, testing, integration testing with external systems, and adherence to corporate security and privacy policies, management of raw datasets of vehicle information.*

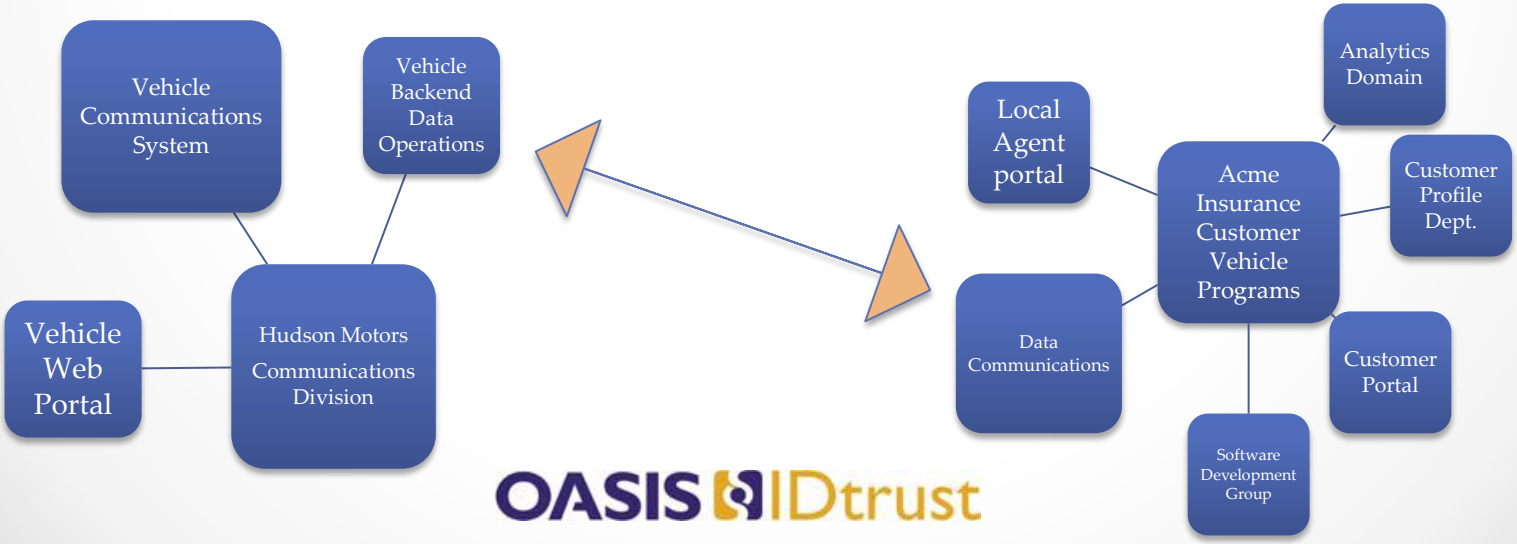




Technical, Managerial and Boundary Data

Data Flows and Touch Points Linking Domains or Systems

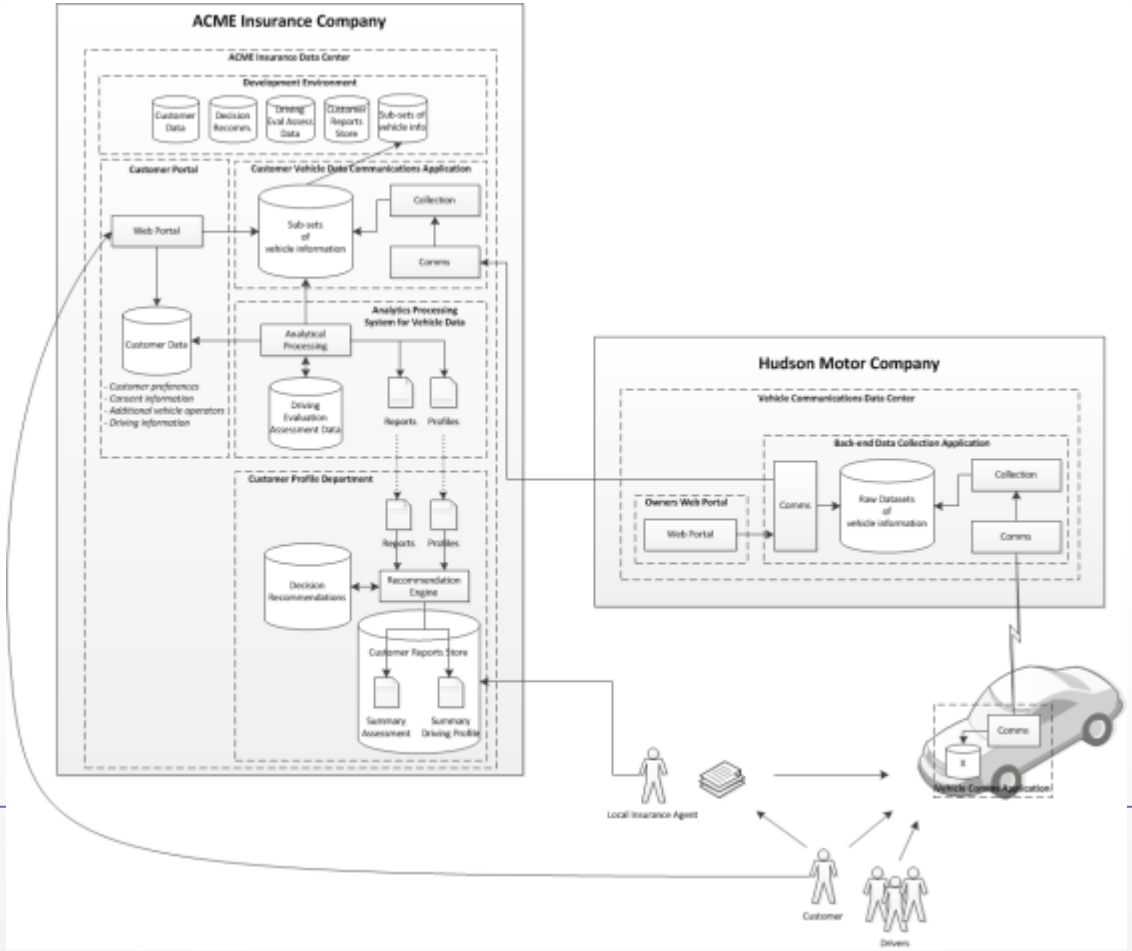
- **Touch points -** the points of intersection of data flows with privacy domains or systems within privacy domains
- **Data flows –** data exchanges carrying PI and privacy policies among domains in the use case



OASIS IDtrust

Technical, Managerial and Boundary Data

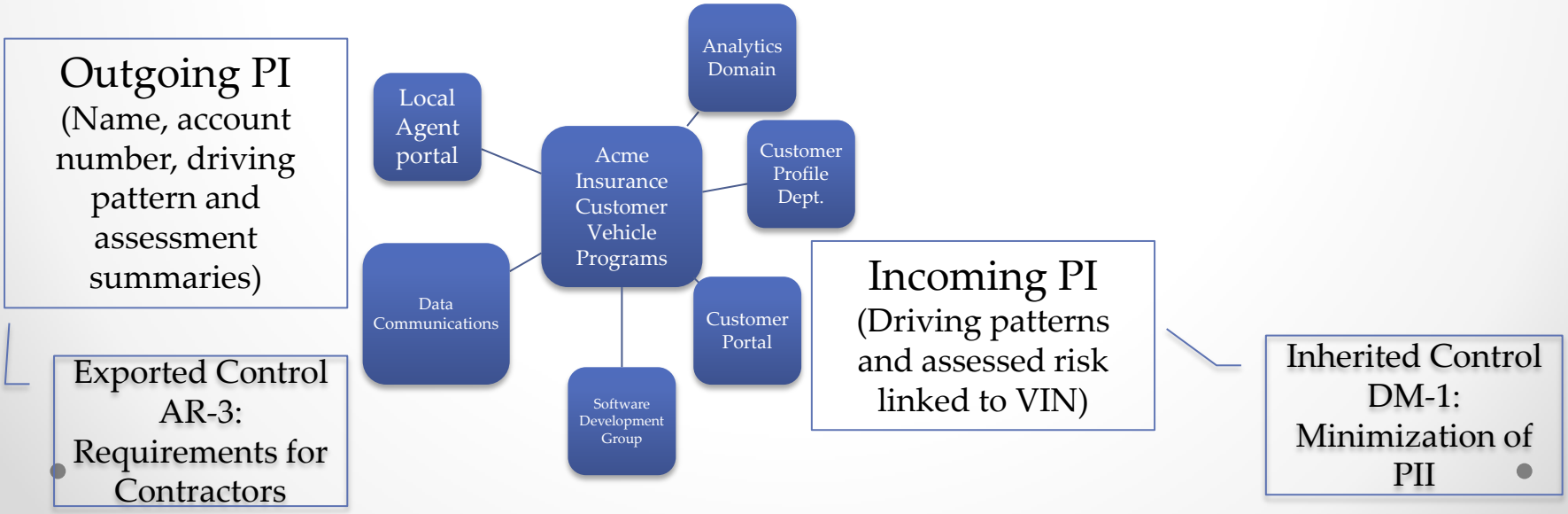
Systems supporting the Use Case applications



Policies, Controls and Supporting Services/Functions

Privacy controls required for developer implementation

- **Control** - a process designed to provide reasonable assurance regarding the achievement of stated objectives
  - per specific domain, system, or applications as required by internal governance policies and regulations
  - including inherited, internal and exported privacy controls



Policies, Controls and Supporting Services/Functions

↳ Services

- **Service** - a collection of related functions and mechanisms that operate for a specified purpose
- **Identify Services satisfying privacy controls**

Core Policy Services	***Privacy Assurance Services***	***Presentation & Lifecycle Services***
Agreement Manage and negotiate permissions and rules	V… Check PI	…ertification Check credentials	Interaction Information presentation and communication
Usage Control PI use	Security Safeguard privacy information and operations	Enforcement Monitor and respond to a…	Access …iew and propose changes to stored PI

Exported Control AR-3: Requirements for Contractors

Inherited Control DM-1: Minimization of PII

Policies, Controls and Supporting Services/Functions

Functions

- Define technical functionality and business processes supporting selected services

- ***Inherited Control DM-1: Minimization of PII***
  - ***Usage service***
    - *Automated interfaces to maintain separation of data using identifier with relatively inaccessible auxiliary info*
  - ***Security service***
    - *Role-based access control*

- ***Exported Control AR-3: Requirements for Contractors***
  - ***Agreement service***
    - *Chain-of-trust contract clause*

"Responsibilities" Table

Stake-holders/Lead	Use Case Descrip-tion	Applications	Data Subjects	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

A Work in Process

- PbD-SE TC and PMRM TC working in parallel to develop practical standards and standards-derived tools
- Open to broader participation from business, policy and technical experts
- Contact today's workshop speakers or email: join@oasis-open.org

OASIS IDtrust