Security in knowledge

OASIS Privacy Management Reference Model (PMRM)

Dr. Michael Willett

OASIS and WillettWorks

OASIS = Organization for the Advancement of Structured Information Standards

ABSTRACT

- **The Privacy Management Reference Model and Methodology (PMRM) supports: understanding and analyzing privacy policies and their privacy management requirements in defined use cases; and selecting the technical services which must be implemented to support privacy controls. Keenly relevant when personal information (PI) flows across regulatory, policy, jurisdictional and system boundaries.**

- https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm
  Published Specification from the OASIS PMRM Technical Committee

ABSTRACT

- The Privacy Management Reference Model and Methodology (PMRM) supports: understanding and analyzing privacy policies and their privacy management requirements in defined use cases; and selecting the technical services which must be implemented to support privacy controls. Keenly relevant when personal information (PI) flows across regulatory, policy, jurisdictional and system boundaries.

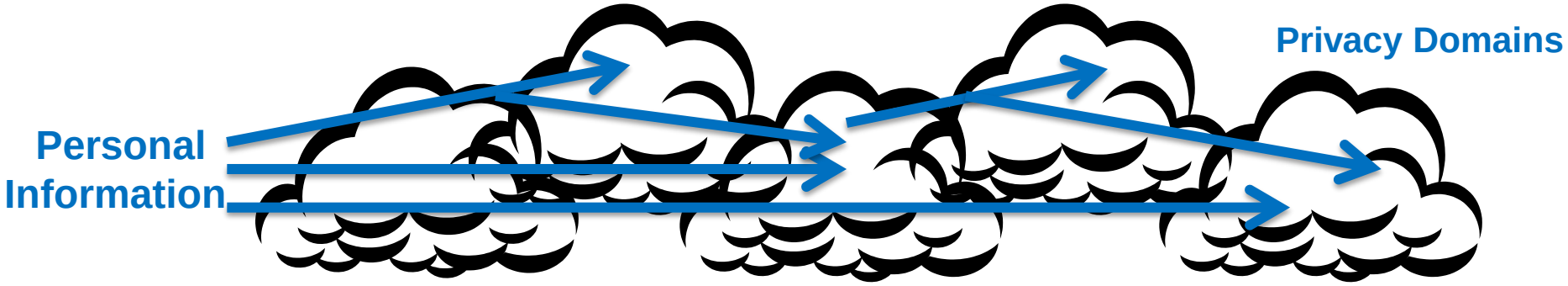
Conceptual model of privacy management

Methodology for analyzing privacy Use Cases

Set of operational **Services**: map privacy requirements to Services

- https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pmrm
  Published Specification from the OASIS PMRM Technical Committee

Operational Privacy Management



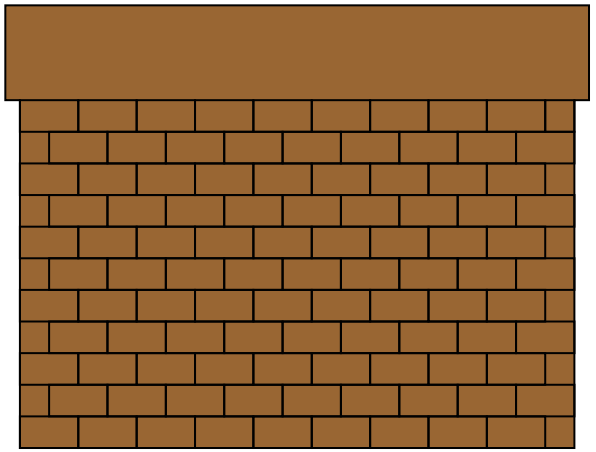
- From an operational perspective: **privacy management** is the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) throughout its life cycle
  - consistent with data protection principles, policy requirements, and the preferences of the individual
- *Proper* and *consistent* must apply throughout the PI life cycle
  - apply to all actors who have a connection with the information
  - apply to all systems/networks and jurisdictions where PI information is exposed

From Privacy Requirements to Privacy Management

Privacy Requirements

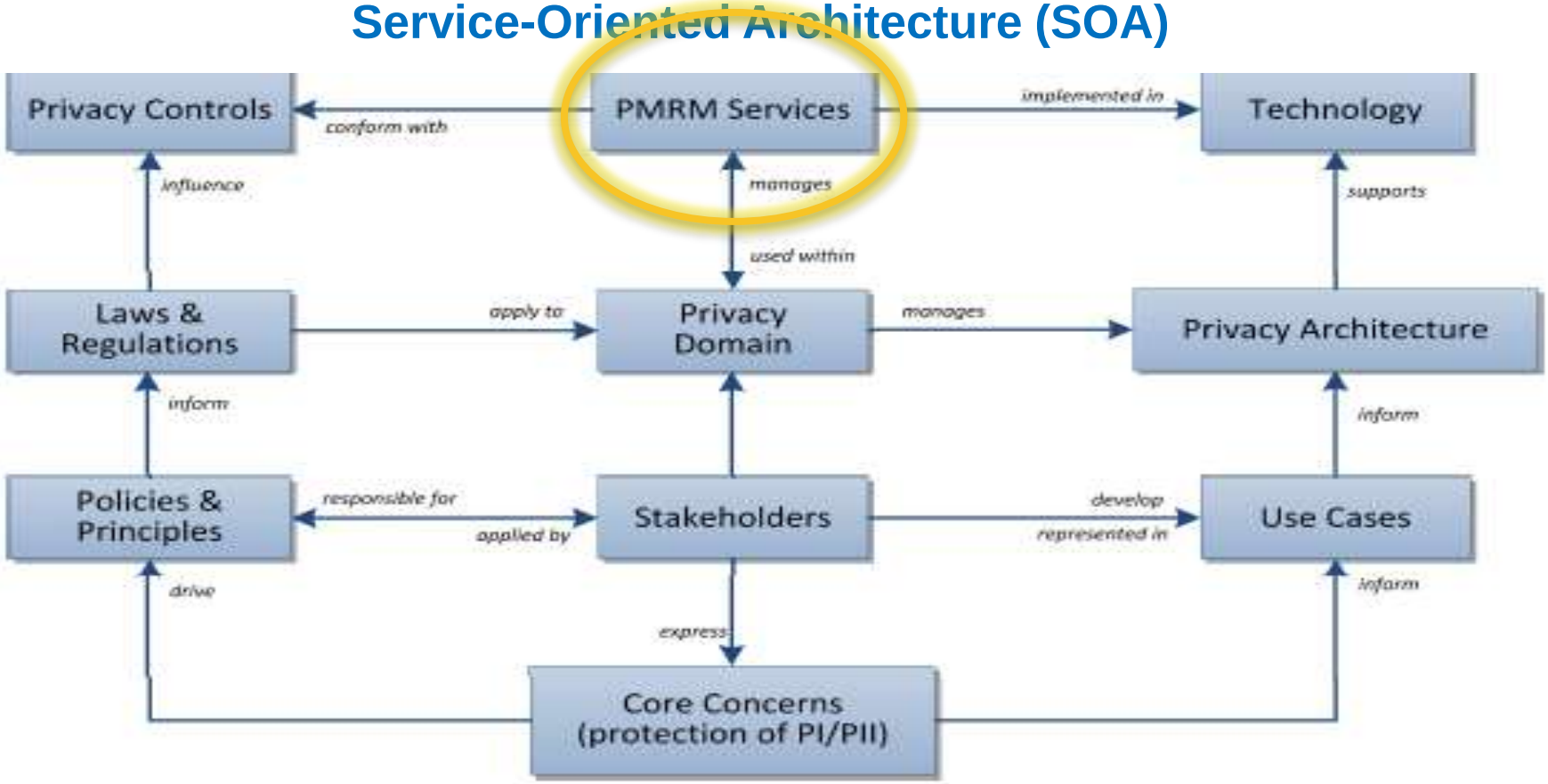
Methodology/Analysis

Services



Privacy Architecture

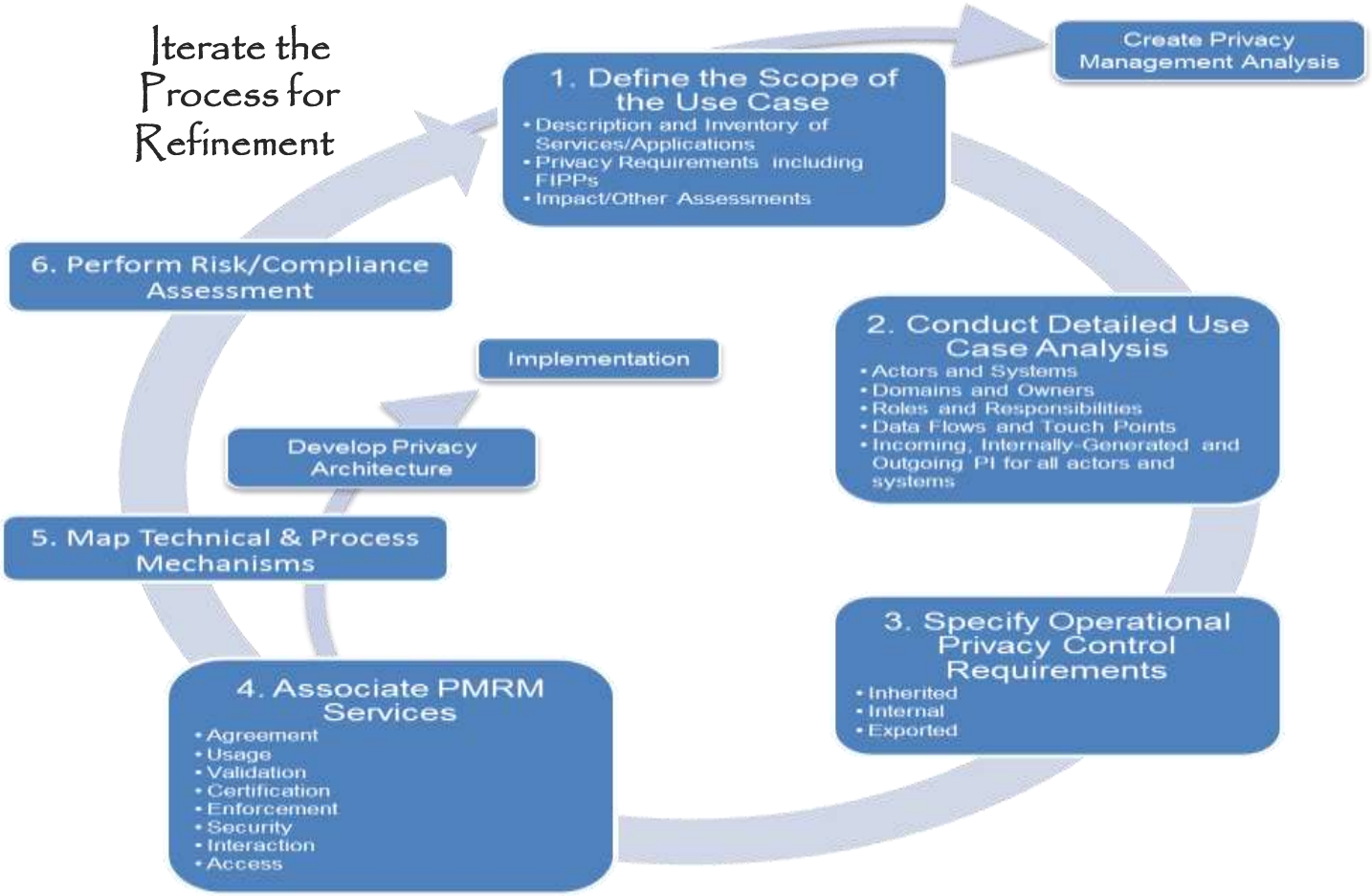
PMRM - Conceptual Model



- The model provides a common conceptual framework and vocabulary to help people cooperate across disciplines and organizational boundaries...

PI = Personal Information PII = Personally Identifiable Information

PMRM - Methodology



- ...and the methodology provides a common set of tasks to achieve a privacy architecture and privacy management analysis

Methodology: 18 Tasks

1. Use Case Description
2. Use Case Inventory
3. Privacy Policy Conformance Criteria
4. Assessment Preparation
5. Identify Actors
6. Identify Systems
7. Identify Privacy Domains and Owners
8. Identify roles and responsibilities within a domain
9. Identify Touch Points
10. Identify Data Flows
11. Identify Incoming/Internally Generated/Outgoing PI
12. Specify Inherited Privacy Controls
13. Specify Internal Privacy Controls
14. Specify Exported Privacy Controls
15. **Identify Services that conform to identified privacy controls**
16. **Identify Functions that satisfy selected Services**
17. **Conduct Risk Assessment**
18. Iterate the analysis and refine

ANALYSIS

Implementation Design

Fair Information Practices/Principles (FIP/Ps)

"BRICKS"

- FIP/Ps
- Comprehensive privacy requirements
- Legislation
- Regulations
- Privacy policy
- Ad hoc "solutions"
- …

Accountability
Notice
Consent
Collection Limitation and Information Minimization
Use Limitation
Disclosure
Access and Correction
Security/Safeguards
Information Quality
Enforcement
Openness
……
Anonymity
Information Flow
Sensitivity

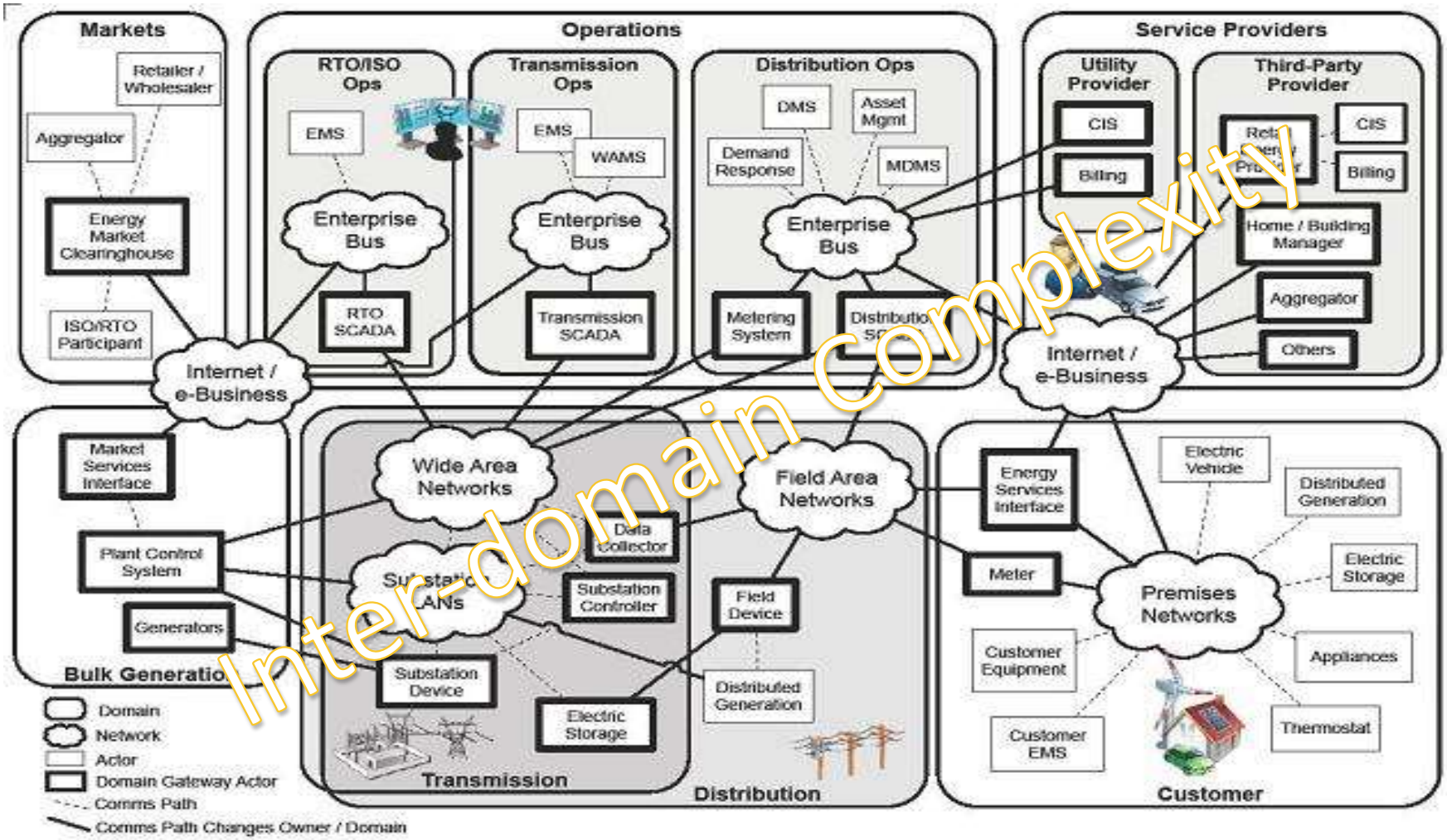
PMRM Services (8)

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

PMRM Services

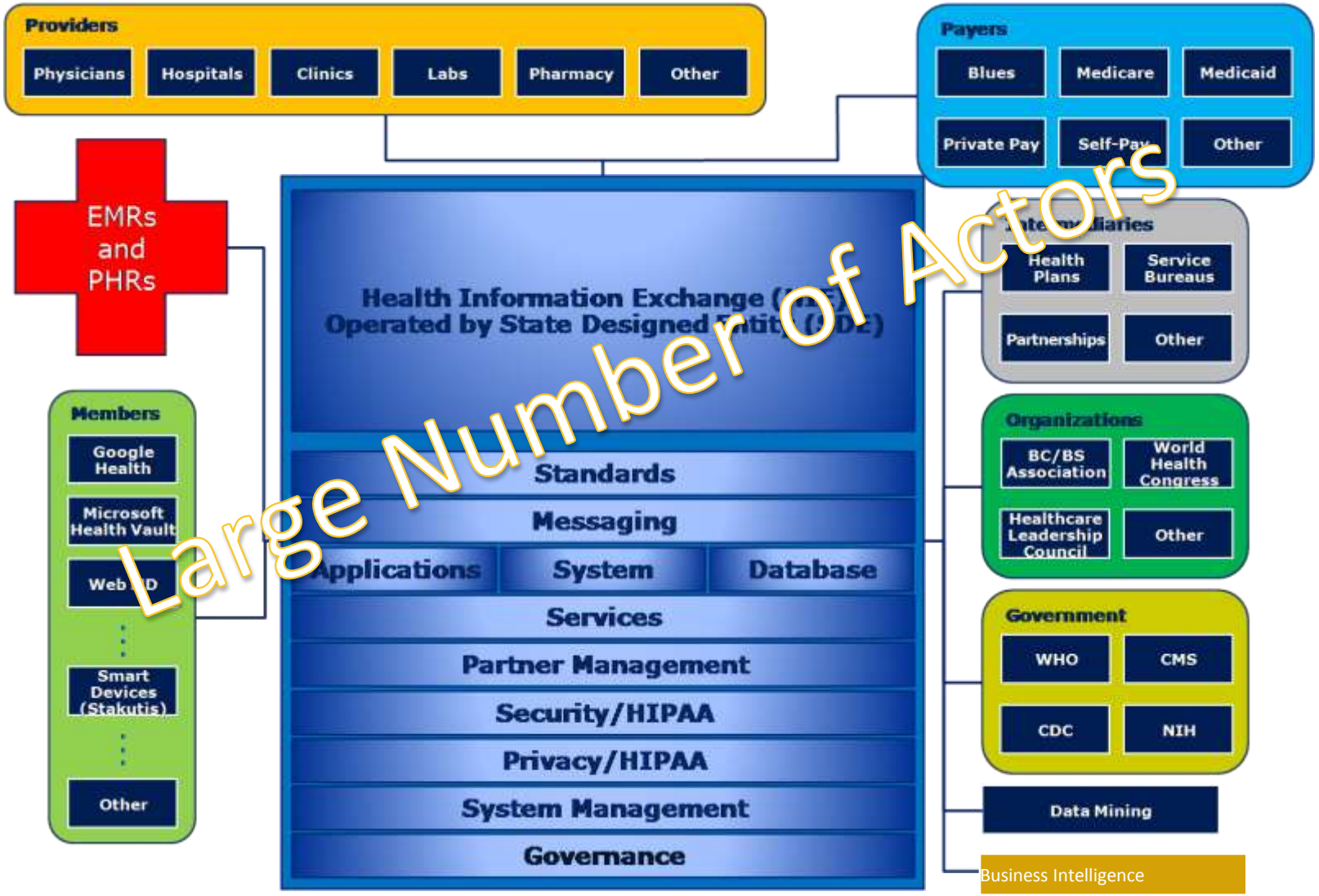
SERVICE	INFORMAL DEFINITION	FUNCTIONALITY
AGREEMENT	Manage and negotiate permissions and rules	Define and document permissions and rules for the handling of PI based on applicable policies, individual preferences, and other relevant factors; provide relevant Actors with a mechanism to negotiate or establish new permissions and rules; express the agreements for use by other Services
USAGE	Control PI use	Ensure that the use of PI complies with the terms of any applicable permission, policy, law or regulation, including PI subjected to information minimization, linking, integration, inference, transfer, derivation, aggregation, and anonymization over the lifecycle of the use case
VALIDATION	Check PI	Evaluate and ensure the information quality of PI in terms of Accuracy, Completeness, Relevance, Timeliness and other relevant qualitative factors
CERTIFICATION	Check credentials	Validate the credentials of any Actor, Domain, System or Subsystem, or system component involved in processing PI; verify compliance and trustworthiness of that Actor, Domain, System or Subsystem, or system component against defined policies
ENFORCEMENT	Monitor and respond to audited exception conditions	Initiate response actions, policy execution, and recourse when audit controls and monitoring indicate that an Actor or System does not conform to defined policies or the terms of a permission (agreement)
SECURITY	Safeguard privacy information and operations	Provide the procedural and technical mechanisms necessary to ensure the confidentiality, integrity, and availability of personal information; make possible the trustworthy processing, communication, storage and disposition of privacy operations
INTERACTION	information presentation and communication	Provide generalized interfaces necessary for presentation, communication, and interaction of PI and relevant information associated with PI; encompasses functionality such as user interfaces, system-to-system information exchanges, and agents
ACCESS	View and propose changes to stored PI	Enable data-subject Actors, as required and/or allowed by permission, policy, or regulation, to review their PI that is held within a Domain and propose changes and/or corrections to their PI

NIST Smart Grid Conceptual Model



Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0

Networked Health I.T.



DO NOT TRACK (DNT) Use Case

Security in knowledge

DNT Use Case (abbreviated)

- **Do Not Track (DNT) broken down into two distinct (T) phases:**
  - ***Tracking*** (often called ***Collecting***): For purposes of market research, recording the associated data (site, request, etc) when a consumer visits web sites, using tracking cookies and other techniques.
  - ***Targeting***: Creating behavioral advertising from the tracking data and presenting such to the consumer.

Visited web sites are called **1st parties** and the creator of targeted advertising is called a **3rd party**.

Basic inventory for the DNT Use Case:

Consumer (C)
Consumer browser (B)
Target web site (1st)
Third-Party "tracking" web site (3rd)
Legislation (L)
Enforcement authority (E)
Technical Standards (eg, HTTP header for Do Not Track) (T)

DNT Use Case: … Task 15 (Services)

C – B: Set Consumer DNT preference

Consumer	Browser
Initialize browser	
	INTERACTION (agent): Display DNT preference-setting page with clear definitions to the Consumer
Set DNT preference	
	INTERACTION: Confirm DNT preference with Consumer; send DNT preference to USAGE.
	USAGE: store DNT preference in secure storage

B – 3rd: Consumer DNT preference; if DNT = OFF: NO: tracking/collecting information

Browser	3rd party tracking site
INTERACTION: Browser retrieves DNT preference from USAGE	
Consumer request to 1st party site, carrying the DNT preference in the HTTP header	
	INTERACTION: 1st and 3rd party liaison: Consumer request shared with 3rd party, including DNT preference
	INTERACTION (agent): extract DNT preference from request
	If DNT = ON: USAGE: Store the DNT = ON agreement
	If DNT = OFF: INTERACTION: send a tracking cookie to the consumer browser (INTERACTION agent) for installation USAGE: Store the DNT = OFF agreement

B – E: notice of any regulatory violations (Enforcement can have a local browser component)

INTERACTION: monitor for tracking cookies. If tracking cookies appear and DNT = ON, send alert notice to ENFORCEMENT: send violation notice to the Enforcement authority with 3rd party Identifying PI Note: Techniques other than tracking cookies could be used to track/collect the consumer	

3rd – E : log/audit compliance with consumer DNT preference

Summary

- Privacy management “state of the art”: Requirements expressed in FIP/Ps, legislation, regulation, or policy, but without a supporting “system design”
- PMRM Specification available from OASIS
- Model and Methodology applicable to real Use Cases
- Purpose: Analyze privacy requirements and transform to operational Services; ie, “solve” privacy management
- Next steps: Field test the PMRM/Methodology with Use Cases through Workshops
- Join us!

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