PMRM TC Meeting  
May 22, 2024  
Agenda  

• Welcome and introductions  
• Status of the PMRM TC and recent work with ISO  
• Overview of PMRM and the new ISO/IEC27561 standard  
• New Members – Royal Holloway, University of London  
• TC Workplan Opportunities and Discussion  
• Chair and co-Chair election  
• Other business  
• Adjourn
From PMRM TC Scope

• Define a set of operationally-focused privacy requirements which can serve as a reference for evaluating options for designing and implementing operational privacy controls. These requirements will constitute a useful working set of ‘privacy guidelines’, which can both serve as general guidance, and as a feature set against which the PMRM and any implementation can be tested.

• Define a structured format for describing privacy management services, and identify categories of functions that may be used in defining and executing the Services.

• Define a set of privacy management Services to support and implement the privacy requirements at a functional level. These Services will include some capabilities that are typically implicit in privacy practices or principles (such as policy management or interaction), but that are necessary if information systems and processes are to be made privacy configurable and compliant.

• Establish an explicit relationship between security requirements and supporting security services (such as confidentiality, integrity and availability services) and the privacy management Services. Security services and standards are essential to secure Personal Information; therefore, each specific privacy management Service is expected to have its own security service requirements.

• In order to refine the Privacy Management Reference Model, the TC may employ and refine use cases supplied by other OASIS TCs and external organizations. The TC may also consider hosting educational workshops and producing additional supporting materials such as ‘best practices’ documents.
PMRM Status – Recent Work with ISO

• Formal liaison with ISO/JTC1/SC27, WG5 since 2019
• Focus on advancing PMRM as an ISO standard
• Initial Study Period
• Integration with other ISO standards
• Finally published after 4+ years
• Important Work Can be done by the TC
PMRM and POMME – Privacy Engineering

• Privacy Engineering
  what is it and why is it necessary?

• Standards
  supporting a privacy engineering practice

• Essential Role of the privacy Engineer
  focus on the operationalization of applications, including networked and interdependent apps

• Privacy operationalization analysis
  “use cases” [PMRM] and “targets of analysis” [POMME]

• Multiple stakeholder roles
  “boundary documents” - privacy engineering practitioners, software developers, DPOs, regulators etc.

• Technical tools and schemas
  supporting privacy engineering and lifecycle maintenance analysis
What is needed to achieve trusted privacy and security operationalization...

- detailed understanding of applications including associated processes
- technical, geo, and other domains, organizations, and roles
- application and system interdependencies
- **functional** security and privacy controls
- security and privacy control interdependencies
- operational environments and state
- operational risks
- application lifecycles
- A lot of documentation (and meta data)
Why TC Engagement Important:
Privacy Engineering supports trusted data protection operationalization
Including research and analysis of interdependent applications, devices, systems, and associated control requirements...
Privacy Engineering-Focused Standardization

supports management of complex, real-world scenarios in both PMRM and POMME

- Primary focus on data protection/privacy for **defined and well-bounded analytic use cases** (targets of analysis) – not simply abstract policy or regulatory requirements
- Supports evaluation of **existing apps** and systems at **all stages of lifecycle**
- Integrates privacy **and security** control requirements
- Provides a model and methodology to discover, **evaluate, and document** all aspects of data protection - from policies, to controls, to functional implementations and interdependencies
- Provides **standardized, structured, reusable data artifacts enabling lifecycle management** - valuable to the business, data subjects/PII Principals, developers, consultants, certification bodies, conformance assessors, etc. as appropriate
- Supports **development of technical schemas and tools**
- **Is permissive** – the scope and level of effort and detail to analyze use cases is determined by the entity commissioning the analysis
PMRM and Privacy Engineering

The PMRM V1.0 CS02 - A methodology and analytic tool developed to:

- enable the structured analysis of “use cases” in which personal information (PI) and PII are used, generated, communicated, processed and stored and erased
  - Support for applications, IoT, Cloud, complex hyper-connected systems, as well as smaller components of a system

- show the linkages among data, data flows, PI, privacy [including security] policies, privacy controls, privacy-enabling Services/functionality, and risk

- Integrate with and support existing privacy standards

- achieve data protection by design requirements and compliance across policy and system boundaries

- A “boundary document” supporting multiple stakeholders

http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html
POMME and Privacy Engineering


- Builds on PMRM terminology and concepts -- http://docs.oasis-open.org/pmrm/PMRM/v1.0/cs02/PMRM-v1.0-cs02.html

- More detailed, with multiple modifications, including
  - Maps POMME to ISO/IEC 29100:2023 privacy principles
  - More structured approach – “Processes, Activities, and Tasks”
  - Stronger linkages and references to other standards
  - New illustrations and tables
  - Complete integration of privacy controls and security controls
  - Terminology changes: PMRM “Services” now “Capabilities”
  - Eliminates embedded running use case -- but includes SDLC, ISO/TR 31700 Use Case
  - Detailed glossary and bibliography
PMRM TC Workplan Opportunities

• Reinvigorate tool development – **applicable to both PMRM and POMME**
  • Graf database approaches to manage data
  • Schemas
  • Integration with other standards or industry initiatives such as MITRE’s ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework

• Podcast or Webinar tutorials - focus on privacy engineering using PMRM and POMME

• Industry or technology-focused initiatives such as:
  • AI
  • Use Cases
  • CMM and privacy

• Conference, workshop and event outreach and marketing projects

• Other…