Introduction:

First and foremost I applaud your work. If PbD and the PMRM is to become a reality it must be formally integrated into the IT and business process engineering development processes.

Developing a methodology that produces a set of controls and hence services/mechanisms that are to be implemented by Software Engineers is extremely difficult.

It also comes at a time where the evolution of the Privacy Office has not reached a mature state according to some of the research I have read.

At the end of this document I share my frame of reference as a privacy professional so that you might take my observations in context. I have divided my observations into two categories: those related to PRIPARE and those related to the PMRM/PbD.

High-level general observations of PRIPARE:

* aligns itself with software development methodologies that software developers are familiar with
* applies the elements of the PMRM and PbD into it’s methodology
* recommends current privacy design tools into it’s methodology, in line with the PMRM and PbD principles
* adds steps to its methodology that high light certain Services helping to ensure that those Services are properly implemented (aka Validation may equate to the Enforcement Service)
* aligns itself with the upcoming legislation in the EU and legislation elsewhere, especially with the incorporation of PbD and Accountability requirements that are present in the GDPR
* implicitly identifies the need for a new privacy professional: the Privacy Engineer that works with the Privacy Office to define granular Privacy Controls and works with IT counterparts to translate them into Services that are implemented as mechanisms in applications
* has identified the need for the PMRM to further clarify Chapter 4 of the PMRM to aid the Privacy Engineer in his/her job and to ensure that the Services definitions are complete and have incorporated the evolving privacy terminology, aka Accountability
* Appendix C represents to me a very comprehensive set of high level generic requirements that the Chief Privacy Officer, the Privacy Office and the Privacy Engineer would have developed for their corporation before the onset of an IT project. It would be of significant benefit that they be translated into Control Statements
  + I recommend that this appendix be republished as a set of Controls following the NIST Security and Privacy Controls Appendices
  + I expect that Appendix C is more comprehensive than the NIST Appendix J
  + Doing so will provide Data Privacy Officers with a beginning point to tailor their corporations’ Privacy Controls. This will go a long way towards jump starting a much more granular approach to data protection, not only in the EU, but globally
  + I am certain that you have done an extensive study of the comprehensiveness of your research, however, releasing Appendix C for comment alone might be beneficial prior to translating it into a set of Controls, using the PMRM definition of Controls.
  + I expect these Controls will need to become more specific as the Privacy Engineer works with the Project Manager and Team as they follow each phase of the PRIPARE methodology. The result may be an ever evolving corporate set of Controls that the Privacy Office maintains as ‘official’ much like the Security Office hopefully does.
  + I would keep these Controls, policy and technology independent, if possible and wait for the development of Services to make them technology specific.
  + For each project, the relevant Controls will be selected and changed to specifically support the product, project, software and operations.
  + The project’s task is to translate its Controls into Services, which in turn are packaged into mechanisms.
  + When one considers the current numbers of security mechanisms related to the current privacy mechanisms, the privacy IT community has miles to go. I recommend that PRIPARE demonstrate with multiple examples the transition from Controls to Services to Mechanisms. Doing so will jump start the IT community in understanding how to make that transition.
  + In addition, the Privacy Engineer would in turn update the corporation’s generic Controls for the next project and would also keep a running set of more specific Controls, Services and Mechanisms to be used in the next projects

PRIPARE observations relative to the PMRM and PbD:

* PMRM is meant to be an iterative and comprehensive model and methodology, which means:
  + Early passes through the methodology at the onset of a corporate privacy program or a new company product idea produces high level controls and influences the overall privacy and IT architectures and the actual company product design.
    - I recommend the PMRM be integrated into PRIPARE at its earliest phases, perhaps at each phase, beginning with 6.3.1.
    - In 6.3.1 the PSMOs would have already developed high-level controls using the PMRM and it would be in this phase that the Privacy Engineer would execute the PMRM Chapters 2 and 3 at a high level to confirm that each domain is meeting the high level privacy Controls with the project team and the guidance of the PSMOs.
    - I recommend in 6.3.1.2 the growing list of privacy controls and services and mechanisms be integrated into a targeted Software Engineer program by the Privacy Engineer. See comments above.
    - I recommend that you consider separating **models and frameworks** from tools and technologies that implement the models and frameworks.
    - I recommend that you consider adding to the blue inserts a horizontal bar at the bottom above tools and techniques that would refer to the **models and frameworks** that have influence the selection of tools and techniques. For example a PIA is a technique that might include all of the elements of the PMRM and PbD. The PMRM and PbD are the models and frameworks.
    - I also recommend, given you are going to keep these blue inserts that you consider in the inputs adding some of the PbD and PMRM terms, such as Privacy Controls in and Privacy Controls and Services out and Services in and Mechanisms out, starting with page 33.
    - You might also consider reviewing the comprehensive PbD document list and PMRM to strengthen the inputs and outputs to make them more granular.
    - I’d revise the Processes to match either PbD/PMRM and/or the tools.
    - I like these inserts and think they are valuable
    - I would also consider adding the Privacy Engineer to the Suppliers

***Note: it is at the beginning phase 6.3.1 that major changes are best made to avoid significant rework later. Once domain boundaries and flows are set I’ve found that it is almost impossible to change them***

* + Subsequent passes refine the controls, continues to tweak the privacy and IT architectures and most importantly impacts the structure of the business processes and what application and/or domain is to do what
    - At each subsequent phase I would include the PbD and PMRM. The tools and techniques will change but the overarching model and frameworks will remain the same.

***Note: I did not research Patterns. Is it a tool/technique or a model/framework?***

* Highlighting Privacy Control examples, as defined in the PMRM is critical as you take the implementation of Privacy to a MUCH more granular level. When I think of the Privacy Controls I gave to IT they were extremely high level. For example, the control that requires consent before personal information is collected, opened up the conversations around is the ip address personal information? Naturally this Control needs to be much more specific for an IT developer. It becomes many Control statements, each with a corollary one for Marketing. There are so many Controls that are either not 100% implementable or detract from the user experience.
  + I recommend in your example that you demonstrate increasingly granular Controls and Service/Mechanisms at each phase. That will go along way to help readers see the PMRM and PbD in action.
* Services vs Mechanisms. We had a bit of discussion about this at the last PMRM meeting. I have been slow to adopt Services. I may still not understand them fully. I have always had trouble with the Services names as they were not familiar terms.
  + In simple terms, I now look at the Services as a check list when implementing a privacy Control
  + Once I have completed reviewing each Control, I might package Services into Mechanisms. Those Mechanisms may live together in an application or may be modularized
  + I do think that once a set of Controls are implemented into Mechanisms using the Services as guidance, the privacy implementation will be complete

***Note: This certainly requires more discussion at our next PMRM meeting using privacy, not security examples. I personally look forward to your revisions of PRIPARE and your interpretation***

* It would be an interesting exercise to map the categories you use in Appendix C to the eight Services to confirm that the categories and the Services are comprehensive and their definitions complete.
* Accountability is a key requirement, especially in the EU. The demonstration of Accountability might be clarified in the description of the PMRM Enforcement Service. Naturally, the demonstration of Accountability would in turn require that the implementation of the 8 Services include an ability to demonstrate Accountability. If this is so, is the Validation phase synonymous with ‘Demonstrating Accountability’?
* The Linddun is an interesting document. It may become an additional model/framework or tool or technique to assist PRIPARE in identifying Controls. The last pages of misuse examples might easily be translated into Controls.
* The chart on page 20 seems to mix models/frameworks with tools, if you agree that PMRM/PbD are models/frameworks and PIA is a tool. You might consider simplifying the chart.
* When I reviewed the chart on page 31 and 32 I checked all the PMRM columns on page 31 and 7 more on page 32. I did not check privacy implementation, the first two under release, the first one under maintenance and the decommission item. If the PMRM is integrated into all phases of PRIPARE via tools, it becomes more comprehensive that identified in this chart.
* The first column of the chart on page 62 seems incomplete to me. I was somehow wanting that column to be the comprehensive list of Controls.
* The chart on page 65 seems to be different than the previous discussions.
* I like the discussions of top-down and bottom-up designs. There may be a third category, which starts of top-down and then makes a leap to key bottom-up designs. Often privacy is so complicated that it is easier to make that leap rather than to unpeel the entire onion.
* Appendix C is VERY valuable

Gail’s frame of reference:

Here are some comments that describe how I came into privacy. It might help those reading this understand my comments. I am not a standards developer, but an implementer of standards real time in methodologies that I have created.

After many years in IT development and management, I began my privacy career in 1997 as the first CPO of Bank of America. From Bank of America In 1999 I joined the ranks of privacy consultants in IBM/Fiderus/EDS. In 2004 I joined Manpower as their Global Privacy Director brought in to build its global privacy program. In 2009 I formed Gail Magnuson, LLC and supported Nymity as Research Alliances Director and have an ongoing role that continues to develop many of the templates within the Nymity Accountability Framework Privacy Management Activities supporting the Privacy Office.

I have supported the ISTPA and PMRM initiatives from the beginning and have integrated parts of the PMRM in every methodology I developed and engagement I led as best I could.

I have developed and upgraded over five privacy methodologies and a similar number of self-assessments and audit tools and naturally risk management tools. Naturally these methodologies were put to immediate use for my companies and clients.

In my IT career I integrated the information management works of John Zackman while developing a Bank Systems Architecture and methodology for First Union Bank in collaboration with ten of the larger financial institutions in the United States

My interests in standards and methodologies have always been to use them for the benefit of my clients and companies.

The boundaries or scope of my privacy initiatives were mostly corporate wide, often global and top down. My challenge was to set broad strategy, policy, guidelines, controls and sample services or mechanisms that could be used throughout the corporation and leveraged by many in operations and IT.

These privacy initiatives often resulted in major changes to the flows of personal data and what personal data was managed by which domains, IT applications and business processes. In other words, using the PMRM methodology, I was able to change the product designs and IT and business process architectures. Such broad brush recommendations made a profound impact on ensuring privacy compliance for the entire corporation.

Detail Research:

**PMRM Control:** A process designed to provide reasonable assurance regarding the achievement of stated objectives

**NIST Sample Privacy Control:**

TR-1 PRIVACY NOTICE

Control: The organization:

a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;

b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and

c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Supplemental Guidance: Effective notice, by virtue of its clarity, readability, and comprehensiveness, enables individuals to understand how an organization uses PII generally and, where appropriate, to make an informed decision prior to providing PII to an organization. Effective notice also demonstrates the privacy considerations that the organization has addressed in implementing its information practices. The organization may provide general public notice through a variety of means, as required by law or policy, including System of Records Notices (SORNs), Privacy Impact Assessments (PIAs), or in a website privacy policy. As required by the Privacy Act, the organization also provides direct notice to individuals via Privacy Act Statements on the paper and electronic forms it uses to collect PII, or on separate forms that can be retained by the individuals.

The organization Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) is responsible for the content of the organization’s public notices, in consultation with legal counsel and relevant program managers. The public notice requirement in this control is satisfied by an organization’s compliance with the public notice provisions of the Privacy Act, the E-Government Act’s PIA requirement, with OMB guidance related to federal agency privacy notices, and, where applicable, with policy pertaining to participation in the Information Sharing Environment (ISE).124 Changing PII practice or policy without prior notice is disfavored and should only be undertaken in consultation with the SAOP/CPO and counsel. Related controls: AP-1, AP-2, AR-1, AR-2, IP-1, IP-2, IP-3, UL-1, UL-2.

Control Enhancements: (1) PRIVACY NOTICE | REAL-TIME OR LAYERED NOTICE The organization provides real-time and/or layered notice when it collects PII. Supplemental Guidance: Real-time notice is defined as notice at the point of collection. A layered notice approach involves providing individuals with a summary of key points in the organization’s privacy policy. A second notice provides more detailed/specific information.

References: The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), EGovernment Act of 2002 (P.L. 107-347); OMB Memoranda 03-22, 07-16, 10-22, 10-23; ISE Privacy Guidelines.

**NIST Sample Security Control:**

AC-7 UNSUCCESSFUL LOGON ATTEMPTS

Control: The information system:

a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.

Control Enhancements:

(1) UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK [Withdrawn: Incorporated into AC-7].

(2) UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE The information system purges/wipes information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging/wiping requirements/techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts.

Supplemental Guidance: This control enhancement applies only to mobile devices for which a logon occurs (e.g., personal digital assistants, smart phones, tablets). The logon is to the mobile device, not to any one account on the device. Therefore, successful logons to any accounts on mobile devices reset the unsuccessful logon count to zero. Organizations define information to be purged/wiped carefully in order to avoid over purging/wiping which may result in devices becoming unusable. Purging/wiping may be unnecessary if the information on the device is protected with sufficiently strong encryption mechanisms. Related controls: AC-19, MP-5, MP-6, SC-13. References: None. Priority and Baseline Allocation: