In 2007-2008 a group of privacy and HR experts came together to produce “The Use of Employee Information Framework” under my leadership and that of the Ponemon Institute. The overall purpose is highlighted below and the Sample Case as well. What I have done is to correlate how we applied the ISTPA/PMRM work.

Since the first version of the ISTPA/PMRM works, I have applied elements of its model and methodology to the work I have done as a CPO and consultant. I decided to map this initiative as a test to see if I might write a compelling white paper about how I have adopted it and what our collective challenges are as we move forward to making PbD, Accountability further reality.

The Use of Employee Information Framework:

“The Use of Employee Information framework has been developed as a tool through which companies can make decisions in their privacy and security programs relative to the use of employee information. The framework recognizes the complex interactions of information elements, business needs, employee needs and global economic and regulatory considerations and most importantly the business value or context in which a company makes those decisions. Here are some of the demonstrable benefits that have been identified to date.

* Improve information efficiency - Only PI/SPI information minimally required is collected and stored.
* Attainable level of legal compliance - Sharing of PI/SPI information is consistently and legally defined across internal and external business units.
* Improve employee trust – Employee perceptions of SPI information is acknowledged and honored whenever feasible.
* Reduce risk – Privacy related employee information breaches could be minimized.
* Gain workforce flexibility -- Position the enterprise to accommodate the emerging workforce.
* Gain significant innovation without the need of growing a workforce.
* Streamline, automate or eliminate business processes – Elimination of FTE and equipment
* Lower unit costs – Outsourcing and/or off-shoring
* Vendor Information Checklist – Facilitate the management and auditing of vendors

The Use of Employee Information Framework Sample Case: This framework presents a methodology for making important decisions about employee information. The type of relevant decisions can range from the policy (strategic) level to the program (implementation) level. To aid in the understanding of how to use the various elements of the framework (illustrated below in Figure 1), we have posed a sample case to show how the framework can be used to arrive at a decision. The sample case along with five possible solutions is outlined in the box at the end of this section. There is a dialogue box within each of the subsequent sections to illustrate how that section can be used to further the decision making process.

The Draft Mapping of the PMRM Tasks to the Use of Employee Information Framework:

| PMRM | Use of Employee Information (EI) Framework | Comments |
| --- | --- | --- |
| Task #1: Use Case Description | Task #1: Use of Employee Information Framework Overview – Sample Case |  |
| Task #2 Use Case Inventory | Task #2: List and group into Categories the following: Employee Data Subjects; Business Entities that govern, collect, use, share and/or transfer EI; the Media used, such e-mail, phone, et.al; EI Categories and detail EI; Business Processes: Employee Processes; Employee Needs. Identify survey information to be used in Task #3  Task #4: The Context: Meeting the Privacy and Security Needs of the Total Workforce by documenting the relevance to the new age and upcoming/future employees, trends in the workplace and the relevance of it all to the Privacy and Security Needs of the workforce. Note that Task #4 was performed after Task #3  Task #5: Identify Internal and External Factors by documenting the impacts of the global economy, the availability of skilled workers and the internal corporate factors using a series of ‘radio dials’ to calibrate corporate culture | Each list included additional documentation, such as definitions, purposes, classification of EI into sensitive or not, et.al. |
| Task #3: Privacy Policy Conformance Criteria | Task #2: Identify the Regulatory Drivers | The Regulatory Drivers included not only global privacy related regulations but Labor, Export, Anti-Terrorism, Employee Monitoring, OSHA, et.al. As this initiative was to create a frame work to develop policy the Conformance Criteria was the regulatory requirements |
| Task #4: Assessment Preparation | See Task #3 where we identified Key Observations | A running set of assessments were identified in the Key Observations |
| Task #5: Identify Participants | See Task #2 Participants were part of the Business Entities |  |
| Task #6: Identify Systems | See Task #2. Systems were part of the Media Used |  |
| Task #7 Identify Privacy Domains and Owners | See Task #2 Domains and Owners were part of the Business Entities |  |
| Task #8: Identify Roles and Responsibilities within a Domain | See Task #2 Roles and Responsibilities were part of the Business and Employee Processes |  |
| Task #9: Identify Touch Points | Task #3: Create a series of Matrices that map Business Process Categories to EI Categories, creating Business Observations; relate Business Processes to Business Observations; relate EI to Business Observations; relate EI to Employee Needs; Employee Needs to EI; Employees’ Perspective Relative to Business Processes; relate Employee Workplace Activities to Business Processes; Business Processes to Laws; Employee Processes to Laws; EI to Laws; | At each mapping, Key Considerations were documented in general, for EI, for Business Processes and for Policy. Many of these Key Considerations are written as possible Controls |
| Task #10: Identify Data Flows | See Task #3 where EI was mapped to Business Processes |  |
| Task #11: Identify Incoming PI | See Task #3 where we identified Business Entities | We did not map Business Entities to Business Processes and Business Entities to EI. If we had we could have identified Incoming, internally generated, and outgoing EI. By identifying Business Entities we did carry our reflections in the Key Considerations, which contain Controls for Business Entities |
| Task #12: Identify Internally Generated PI | See Task #3 where we identified Business Entities | We did not map Business Entities to Business Processes and Business Entities to EI. If we had we could have identified Incoming, internally generated, and outgoing EI. By identifying Business Entities we did carry our reflections in the Key Considerations, which contain Controls for Business Entities |
| Task #13: Identify Outgoing PI | See Task #3 where we identified Business Entities | We did not map Business Entities to Business Processes and Business Entities to EI. If we had we could have identified Incoming, internally generated, and outgoing EI. By identifying Business Entities we did carry our reflections in the Key Considerations, which contain Controls for Business Entities |
| Task #14: Specify Inherited Controls | See Task #3 where we identified Key Observations | Implicit Controls were identified in the Key Observations |
| Task #15: Specify Internal Controls | See Task #3 where we identified Key Observations | Implicit Controls were identified in the Key Observations |
| Task #16: Specify Exported Privacy Controls | See Task #3 where we identified Key Observations | Implicit Controls were identified in the Key Observations |
| Task #17: Identify the Services necessary to support operation of identified privacy Controls |  |  |
| Task #18: Identify the Functions that satisfy the selected Services | See Task #3 where we identified Key Observations | Often specific mechanisms were identified in the Key Observations. We bypassed the Services and packaging Services into Functions and on into Mechanisms. By identifying the Media Types in Task #1, we were able to reflect the need for different controls depending on the Media (e.g. email, in person, in a system, et. al. |
| Task #19: Conduct Risk Assessment | See Task #1 where we identified Key Observations | These Key Observations identified a running list of risks |
|  | Task 6: Synthesis and Business Value and the Final Decision | The Sample Case was to assist a global company in making a decision on how they should structure an employee privacy policy given certain a desire to consolidate EI in one location outside of the EU. The execution of Tasks #1-#5 allowed the company to make an informed decision amongst five different scenarios and to create the policy fully informed by the detail analysis |
| Task #20: Iterate the analysis and refine | We were continually updating the work of Task #1 as we working on Task #3 |  |