Data Privacy Methodology

Operate ➔ Govern

Implement ➔ Discover

Risk ➔ Classify

Governance

Decision rights and accountability frameworks that ensure progress towards the organization’s strategies and objectives.

Tools / Process

- Personal Interviews
- Review of organization artifacts
- Create a Governance Plan/Policy
- Reviews/Gap Analysis

Discovery

Identification of PHI/PNI/CPI in data stores both active and inactive (online/nearline/offline)

Tools / Process

- RSA DLP – Data Loss Prevention Suite
- Exeros
- Data Inventory
Classification

Assignment of a data sensitivity level to data that is created, amended, enhanced, stored, or transmitted.

Public
Private
Sensitive
Confidential

Tools/Process
- Data Classification Policy

Risk Analysis

Determination of the probable frequency and probable magnitude of future loss exists in the classification categories, and what controls need to be implemented to mitigate the risk.

Tools/Process
- FAIR Risk Assessment

Implementation

Identification, implementation and configuration of tools, processes and practices designed to ensure compliance.

Tools/Process
- AD RMS (DRM)
- RSA DLP
- Identity Lifecycle Management (ILM)
- AIG – formerly Whale
- MOSS
- CoreFront
- BizTalk
- Encryption (Whole disk, backups, DBs)
Operating

Ensuring the selected controls are implemented as intended, are effectively managing risk, and the risks haven’t changed.

Tools / Process
• Audits/Assessments
• Analytics
• Monitoring/Logging
• Risk Assessments
Factor Analysis of Information Risk (FAIR)

Loss Event Frequency
- Probable
- Frequency
  - Threat Capability
  - Impact on Business
  - Vulnerability
- Frequency
- Magnitude

Loss Magnitude
- Probable
- Probability of Action
  - Threat Capability
  - Impact on Business
  - Vulnerability
- Probability
- Magnitude

Losses...

- **Primary**
  - Productivity
  - Response
  - Replacement

- **Secondary**
  - Fines/Judgments
  - Competitive Advantage
  - Reputation