

Privacy Risk Assessment – *Global Supermarket Retailer*

BACKGROUND: The Global Privacy Risk Assessment initiative was sponsored by the CIO of a major international supermarket retailer to identify areas of privacy risk to the enterprise in all global operating companies. As the former Director of Information Security for the supermarket retailer and now the Principal of Assurance Point LLC, I designed and implemented the assessment process for this project.

SCOPE: The above initiative called for a process to be designed to assess privacy risk within each supermarket operating company. Privacy assets were identified as those subject to State and Federal laws as well as the Payment Card Industry standard PCI/DSS. A risk assessment process was designed based on the NIST Risk Assessment framework detailed in NIST SP 800-30 and also based on the OCTAVE methodology. Strength of security controls were determined through a baseline comparison to the ISO/IEC 27001:2005 control framework (comparable in scope and detail to the NIST SP 800-53 framework).

KEY FACTORS: There were several key factors to the process design and project execution that contributed to the success of this project:

- It was critical to examine both business processes as well as technical systems as potential sources of risk.
- The business process assessment was performed in facilitated “discovery” workshops with both process owners and doers participating to identify vulnerabilities in the process workflow.
- Cost effective approach – a risk assessment is not an assurance test. Application level assurance testing and network penetration tests were out of scope. Both of these tests are already being accomplished as part of the enterprises existing security program.
- Support of the business process owners. The project was designed to deliver assessment results to each business process owner.
- The deliverables were designed to support a sustainable risk management program.

KEY DELIVERABLES: The deliverables were designed to support a sustainable risk management program with periodic risk assessment renewals. These were delivered to the business and technical system owners as well as an enterprise information risk governance committee.

- Business and Technical System Characterization
- Privacy Asset Inventory
- Threat Taxonomy
- Vulnerabilities impacting each privacy asset
- Existing security controls baseline assessment against the ISO/IEC 27002 standards
- Qualitative Risk Determination (High, Medium, Low)
- Prioritized time bound recommendations to mitigate risk through controls improvements

AssurancePointLLC.com

Security • Privacy • Compliance

Phone: 207-272-6976 Email: twitwicki@AssurancePointLLC.com

P.O. Box 2887, South Portland, ME 04116

