Executive Summary—Key Steps

- Agree on a common framework for the risk-based auditing and monitoring program.
- Assess privacy risks across the enterprise and then prioritize them by looking at the likelihood of occurrence and impact for the organization.
- Develop a risk-based auditing and monitoring plan or integrate into current compliance plan from the identified privacy risk priorities.
- Assure that a management action plan is developed to mitigate risks and/or resolve risks in a timely manner.
- Assess auditing and monitoring process for effectiveness.

Getting Started

In designing the privacy risk-based auditing and monitoring activities, it is important to work closely with the organization’s senior leadership and the board, or committee of the board, to gain a clear understanding of auditing and monitoring expectations and how these activities can be leveraged together to
help minimize and mitigate privacy risks for the organization. The organization’s compliance officer should be included as well to assure that applicable resources are leveraged and auditing and monitoring activities for privacy are not duplicated in the privacy and organization’s overall compliance plan. There may be other functions that might not be represented on the senior leadership team with whom you will want to consider discussing these activities as well.

Processes for establishing the privacy risk-based auditing and monitoring plan should include performing a risk assessment, prioritizing those risks identified and then developing the plan. If privacy is part of the overall comprehensive compliance plan, then it would be considered in the risk prioritization and ranking for the compliance plan. The overall goal of the plan is to perform periodic audits and monitors to determine compliance with respect to applicable regulatory and legal requirements, organizational policies and/or laws. An additional goal of the plan should be to provide assurance that management controls are in place for the detection and/or prevention of noncompliant behavior. Additionally, risk-based auditing and monitoring should include mechanisms to determine that management has implemented corrective action through an ongoing performance management process to address any noncompliance with privacy.

Once the common framework for the risk-based auditing and monitoring program has been established, six key tasks must be performed:

1. Assessment and prioritization of privacy risks;
2. Development of a risk-based auditing and monitoring plan;
3. Execution of the plan;
4. Facilitation of response by management as to corrective action plan to mitigate and/or resolve risks;
5. Follow up action to determine resolution and/or mitigation by management of the risks identified. This might include re-auditing, validation, monitoring or other focused activity to assist with determination of whether the risk has been decreased;