**Big Data Privacy Risk**

Predictive analysis of big data is a tremendous tool when used and applied correctly. The collection of apparently unlinked data is harmless by itself, but its predictive powers can exceed expectations. For example, the health care industry sees value in big data as a predictor of patient behavior and future health. The Google Now service tracks a mobile device user’s location, calendar events, search inquiries and personal preferences. This service predicts a user’s information needs and displays the information on the user’s mobile device. Using the personal data tracked with Google Now and payment card transactions, the health care industry predictive analysis can categorize patient lifestyles as healthy or unhealthy. The predictive analysis may categorize an individual incorrectly based on just one of the tracked parameters. Enterprises want to mitigate this type of risk with appropriate filters and cross checks.

Risk related to big data can be categorized as operational or information technology based. These risk categories can be mitigated with strong governance.

Operational risk encompasses external and internal factors that include geopolitical risk and the rush to satisfy the board and senior management who are eager to get ahead of the competition. Geopolitical risk, which is created by a country’s policies, includes the European Union laws that restrict cross-border sharing and processing, privacy laws that prevent marketing to certain age groups and US privacy laws that prevent the labeling and sharing of personal, private and financial information, which can lead to identity theft and unauthorized transactions. Industry-specific legislation, such as the US HIPAA, can be very complex, and provisions assuming risk transfer may not be clearly documented or enforced. “Data itself does not create value or cause problems; its use does.”

Corporate chief information officers (CIOs) can be pressured by the board and senior management to implement big data to be able to compete before proper risk controls are applied. Ill-conceived application development controls can lead to data leakage and exposure of private data that are not intended to be seen by developers.

Methodologies such as Agile can support a controlled approach to risk while allowing flexibility. Mapping Agile to COBIT 5 can be an appropriate approach to governance, acquisition and development.

IT risk is business risk—specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. IT risk occurs when safeguards are bypassed. For example, an enterprise may acquire software tools because technologists consider them scalable, but not necessarily because the tools meet the needs of those who plan to use them for business analytics. IT operations can be so focused on development and delivery that simple safeguards for capacity planning are overlooked and resources and data are not monitored or properly planned.

Enterprise policies need to ensure that employees keep stakeholder information confidential during and after employment. This risk is increasing especially given that information has become 21st century currency and data brokers are profiting from the sale of information—commonly referred to as data as a service.