Assessing Your Protection of Personal Identifiable Information (POPI)

One of the unintended consequences of the information age is the availability of personal identifiable information (PII). The combination of name, date of birth, and identification number are the “keys to the kingdom” for the purposes of establishing false identity and fraud. Lost laptops, network break-ins, and phishing expeditions have led governmental entities to establish a patchwork quilt of laws requiring custodians of personal information to provide safeguards and assurance that PII is secure.

In this course, we will discuss:
- PII scope and definitions.
- State and federal PII requirements.
- An action plan for compliance.

Where to Find PII
- The porous nature of data storage
- Traditional computing
- Outsourced systems
- Data on the move
- Into the cloud

What Do We Need?
- Establishing criteria
- Defining the compliance universe
- Identifying the legal requirements
- Fulfilling assurance/monitoring requirements Resolution
- Keeping up with changing technology and compliance
- Monitoring and assurance

Action Plan
- Building a framework for PII
- Aggregating compliance requirements
- Implementing security measures

COURSE CONTENT

What Is Personal Identifiable Information (PII)?
- Various definitions
- Minimum requirements
- Dynamic framework by locality

The Need for Security Over PII
- Performing a meaningful risk assessment
- Selling the results to management
- Overcoming “not just security”