Implementation Plan

Information security is no longer viewed as just an “IT” issue and successful implementation of information security policies requires all employee involvement and coordination among all departments.



*Information Security Program Implementation Guidelines* document describes suggested phases of implementation:

1. The Board of Directors (BOD) approves an Information Security Policy and Information Security Program (ISP) Implementation Guidelines.
2. The CEO/General Manager establishes an Information Security Steering Committee (ISSC) that shall include staff from Administration, IT, E&O, Accounting, HR, Legal, etc.
3. ISSC will coordinate:
   * Initial assets inventory and data classification  
     (ISPL includes *Data Classification Policy* and *Data Assets Inventory Form*);
   * Risk assessment  
     (ISPL *Risk Assessment Procedure* and *Risk Register Form* can be used to support risk assessment);
   * Gap analysis   
     {PCI DSS (Payment Card Industry Data Security Standard), DOE ES-C2M2 (Electricity Subsector - Cybersecurity Capability Maturity Model) or NIST Cybersecurity Framework can be used for gap analysis which can be conducted internally or by external consultant}.
4. ISSC creates Policies Implementation Roadmap (Roadmap) by assigning priorities for implementing policies and controls.
5. On regular basis (i.e., monthly), ISSC reviews implementation progress and selects the next policies for implementation.
6. On annual basis, ISSC reviews status of ISP and recommends changes to the Roadmap.