***NOTICE****: The following has been provided by WBA committee and section volunteers for use by member banks.   
It should be reviewed and revised as appropriate to the user-bank’s own policies, procedures, and practices.*

**Implementing New Vendors/Technology Programs**

An effective New Vendor/Technology Implementation Program is not “one size fits all” to meet the needs of every lender. This outline is not all inclusive but is intended to provide elements to consider and evaluate in relation to your institution’s policies and procedures. Your New Vendor/Technology Implementation Program should consider several factors such as, the size and structure of your organization, the expertise of your staff, and the volume and types of mortgages originated. Controls must be in place to ensure that your policies and procedures are being followed. Perform periodic reviews of your policies and procedures to determine whether changes are needed.

**Responsibilities of Financial Institution:**

* Have written procedures for new implementation and change management for current vendors and technology
* Periodically review vendors and technology
* Periodic risk rating review for prudential regulator/supervising agency

**Procedures:**

* Gather all pertinent information about the vendor in order to do a risk analysis
  + Request a “Vendor Review Package”
    - Many companies will have this available for potential customers
  + Information should include:
    - Contract
    - Pricing
    - Business W9
    - Vendor contact information
    - Insurance (when applicable)
  + Review documentation and disseminate to appropriate parties within the organization
* Risk analysis should consider:
  + Vendor/technology access to customer data
  + Vendor/technology access to bank systems
  + Number of departments or systems the vendor/technology could potentially impact (including business continuity should the vendor/technology become unavailable)
  + Regulations that vendor/technology could impact (including disclosures, privacy, etc.)
* Implementation:
  + Coordinate with all applicable departments
    - Technology that will be housed on bank networks – IT department should be involved to ensure information security is maintained
    - Technology that will be maintained on vendor server – consult IT department for bank requirements
    - Project manager should continue to be involved for testing purposes
      * When possible, submit test information into new system instead of customer information
  + Maintain controls for system
    - Only give access to persons that require vendor/technology to complete their job
    - When possible, give each independent user their own logins and passwords
      * In cases of employee termination, be sure to have administrative access to remove their credentials
    - Monitor system for updates and confer with IT department on network compatibilities
  + Develop internal user guide
    - Guide should include instructions on permissible use of vendor/technology
    - FAQ based on system testing is beneficial
    - Include contact information for vendor/technology and internal employee admin (when applicable) available for questions
  + Train staff