191—90.38(505) Examples of methods of development and implementation. The actions and procedures that follow are examples of methods a licensee may use to implement the requirements of rule 191—90.37(505) to assess, manage and control risks of disclosure:

1. Identify reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems.
2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
3. Assess the sufficiency of policies, procedures, customer information systems and other safeguards in place to control risks.
4. Design an information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the licensee's activities.
5. Train staff, as appropriate, to implement the licensee's information security program.
6. Regularly test or otherwise regularly monitor the key controls, systems and procedures of the information security program. The frequency and nature of these tests or other monitoring practices are determined by the licensee's risk assessment.
7. Exercise appropriate due diligence in selecting service providers.
8. Require service providers to implement appropriate measures designed to meet the objectives of rule 191—90.37(505) and, when indicated by the licensee's risk assessment, take appropriate steps to confirm that service providers have satisfied these obligations.
9. Monitor, evaluate and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of customer information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to customer information systems.