

List A

Methods to Manage and Control Risk

Consider whether the following security measures are appropriate for the credit union to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the credit union's activities. The credit union must adopt those measures it concludes are appropriate.

- *Access controls on member information systems*, including controls to authenticate and permit access only to authorized individuals, and controls to prevent employees from providing member information to people who may try to obtain this information through fraudulent means (i.e., pretext calling);
- *Access restrictions at physical locations containing member information*, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
- *Encryption of electronic member information*, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
- *Procedures* designed to ensure that member information system modifications are consistent with the credit union's information security program;
- *Dual controls procedures*, segregation of duties, and employee background checks for employees with responsibilities for or access to member information;
- *Monitoring of systems and procedures* to detect actual and attempted attacks on or intrusions into member information systems;
- *Response programs* that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies; and
- *Measures to protect against destruction, loss, or damage* of member information due to potential environmental hazards, such as fire and water damage or technical failures.
- *Disposal of information*. Develop, implement, and maintain appropriate measures to properly dispose of member information and consumer information.
- *Oversee Service Provider Arrangements with* appropriate due diligence in:
 - selecting service providers;
 - require service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines; and,
 - where indicated by the credit union's risk assessment, monitor service providers to confirm that they have satisfied their obligations as required by the contract. As part of this monitoring, review audits, summaries of test results, or other equivalent evaluations of its service providers.

The manner of implementing a particular element listed above may vary from credit union to credit union. For example, while a credit union that offers Internet-based transaction accounts may conclude that encryption is appropriate, a different credit union that processes all data internally and does not have a transactional website may consider other kinds of access restrictions that are adequate to maintain the confidentiality of member information.