

Audit Objectives	W/P Reference	Completed By
<p>1. To insure the security and confidentiality of customer records and information.</p> <p>2. To determine that the Bank has established an adequate written Information Security Program.</p> <p>3. To assess the quality of the Banks compliance management policies and procedures for implementing the privacy regulation, specifically ensuring consistency between what the Bank tells consumers in its notices about its policies and practices and what it actually does.</p>		
Audit Procedures		
<p>1. Prior to the audit obtain a listing of vendors from Marketing.</p>		
<p>NOTE: Security of the Banks data can be (is) tested in the physical and logical security of the IS Department review.</p>		
Audit Steps		
A Prior Audit Reviews		
<p>1. Obtain and review prior internal and external audit reports and determine recommendations addressed have been resolved. Review management's response to audit findings.</p>	_____	_____
B Audit Questionnaire		
<p>1. Forward the Privacy of Consumer Financial Information questionnaire to responsible parties. Based on management's response, review the results and conclude on whether generally, the Compliance Officers are well trained and knowledgeable of Gramm-Leach-Bliley Act requirements.</p>	_____	_____
C Policies and Procedures		
<p>1. Obtain a copy of the Banks Privacy Statement and verify it clearly states the following:</p> <p>a. Identifies the information that will be shared;</p> <p>b. Identifies the organizations with which the information will be shared;</p> <p>c. Identifies the purpose for sharing the information;</p> <p>d. Provides a reasonable timeframe for the consumer to opt out.</p>	_____	_____
<p>2. Obtain a written copy of the banks privacy policy or statement that is provided to the bank customers. Verify the privacy statement contains the following:</p> <p>a. A clear explanation of the types of information that the organization collects;</p> <p>b. A brief description of the security measures in place to protect the data;</p> <p>c. A clear explanation of the types of information that are shared;</p>	_____	_____
<p>d. The purposes for which that information is used, and;</p> <p>e. A clear notice of the customer's right to opt out at any time.</p>		
<p>3. Obtain a copy of the banks Information Security program or policy and verify the following:</p> <p>a. The information security program has been approved by the board of directors or an appropriated committee of the board;</p> <p>b. The information security program is appropriate given the size and complexity of the organization and its operations;</p>	_____	_____

AUDIT PROGRAM
EXAMINATION OF: _____

PREPARED BY: Mary Jo Troost
DATE 2003
mtroost@ibcp.com
Independent Bank Corporation

	W/P Reference	Completed By
c. The information security program contains the objectives of the program, assign responsibility for implementation, and provides methods for compliance and enforcement;		

D Risk Assessment/Customer Information	W/P Reference	Completed By
<p>1. Obtain the banks risk assessment process/program for all areas of the bank and verify that all risks and their corresponding impact have been properly identified and that action plans have been appropriately and correctly formulated. Review for the following:</p>	_____	_____
<p>a. It identifies the locations, systems, and methods for storing, processing, transmitting, and disposing of its customer information;</p>		
<p>b. It identifies reasonable foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems and assessed the likelihood and potential damage to the bank and its customers of those threats.</p>		
<p>2. Review the bank's risk management processes for implementing effective measures to protect customer information. Determine the bank considered the following areas, and adopted measures that are appropriate based on risk.</p>	_____	_____
<p>a. Access controls on computer systems containing customer information to prevent access by unauthorized staff or other individuals.</p>		
<p>b. Controls and procedures to prevent employees from providing customer information to unauthorized individuals, including "pretext calling".</p>		
<p>c. Access restrictions to physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.</p>		
<p>d. The encryption of electronic customer information, including while in transit or in storage on networks or systems, in case unauthorized individuals are able to gain access.</p>		
<p>e. Procedures designed to ensure that modifications to customer information systems are consistent with the bank's information security program.</p>		
<p>f. Dual control procedures, segregation of duties, and employee background checks for employees with access to customer information to minimize risk of internal misuse of customer information.</p>		
<p>g. Monitoring systems and procedures to detect unauthorized access to customer information systems that could compromise the security of customer information.</p>		
<p>h. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.</p>		
<p>i. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.</p>		

E Service Providers	W/P Reference	Completed By
<p>1. Obtain a listing of service providers utilized by the Banks'. Judgmentally select a sample of those venders _____ and test for the following vender privacy contract requirements:</p> <p>a. The bank conducted appropriate due diligence in selecting its service providers, taking into consideration information security;</p> <p>b. If contacts were entered into after March 5, 2001, the bank requires its service provider by contract to implement appropriate information security programs and measures;</p> <p>c. The contract adequately prohibits the third party from disclosing or using the information other than to carry out the purposes for which the information was disclosed.</p> <p>d. Where indicated by the banks risk assessment, the bank monitors its service providers to confirm that they are maintaining appropriate security measures to safeguard the bank's customer information (ex: the bank conducts or reviews the results of audits, security reviews or test, or other evaluations).</p>	_____	_____
F. Web Site		
<p>1. Review the Bank's website and verify the following:</p> <p>a. The website includes a privacy statement.</p> <p>b. The website's privacy statement accurately discloses what non public personal information is obtained on the site.</p> <p>2. Determine, through discussion with management, if written procedures are in place for overseeing the website. Verify they include the following:</p> <p>a. For ensuring that new additions to the Website will comply with the existing privacy statement.</p> <p>b. For documenting what changes are made to the Website.</p> <p>c. For recording changes the Website's privacy policies.</p> <p>d. For ensuring that new customer's are informed to the Website's privacy policy in a clear and conspicuous manner.</p>	_____	_____
<p>1. Overall, determine the effectiveness of management controls to ensure compliance with regulatory requirements.</p>	_____	_____
<p>If, as a result of work on this audit, you have changed the nature and extent of tests or you have any suggestions to improve the effectiveness or efficiency of this program, attach a form setting forth your suggestions.</p> <p>_____ suggestions attached</p> <p>_____ no suggestions</p>		