**ANNUAL REPORT ON THE STATUS OF THE**

**INFORMATION SECURITY PROGRAM (SAMPLE)**

From: Information Security Officer

To: Board of Directors

Subject: Information Security Program Summary Report

This summary report will describe the overall status of the information security program and will discuss material matters relating to: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations, and management's response; and recommendations for changes to the Information Security Program.

**RISK ASSESSMENT**

The enterprise-wide risk assessment was updated in June.  The assessment was used to identify and prioritize risks to the confidentiality, integrity, and availability of non-public customer information as well as other critical data. The methodology used is adapted from the National Institute of Standards and Technology.  The assessment involved management and key users to identify critical information assets and corresponding risks to these assets. This assessment was used as the foundation for developing mitigating strategies to manage the specific risks.  All unmitigated risk, those  exceeding the risk tolerance,  were reported to the Executive Committee for acceptance or for additional guidance.

**RISK MANAGEMENT AND CONTROL DECISIONS**

All risks were assigned one of three risk levels as follows:

**Low**: The probability and/or impact of the risk would not significantly disrupt operations or cause significant financial loss.

**Medium**: The probability and/or impact of the risk might disrupt operations and/or cause financial loss.

**High**: The probability and/or impact of the risk would likely disrupt operations and/or cause financial loss.

Given the above definitions, all risks with a residual risk level (after mitigation) of medium or high were submitted to the Executive Committee for review in July. Risk acceptance decisions were made at the July meeting.  In addition, all business unit managers reviewed risk reports related to their respective areas. At this time, there are no unmitigated risks that warrant the board's involvement.

**SERVICE PROVIDER ARRANGEMENTS**

There have been no significant changes to service provider arrangements. Due diligence has been performed for all critical service providers as required by our Vendor Management Program. At this time, there are no significant issues to report.

**RESULTS OF TESTING**

Key controls were tested during the Information Security Audit that was performed in August.  Results of the audit were reported to the Audit Committee. Some employees responded to forged emails. Since the testing, additional employee training has been conducted.

**SECURITY BREACHES OR VIOLATIONS**

No security breaches have occurred at our institution. However, a primary card processor did have an issue that impacted many of our customers.

**Management's Response to Security Breaches or Violations**:  We issued new debit cards to our entire customer base.

**RECOMMENDED CHANGES TO THE INFORMATION SECURITY PROGRAM**

There are no significant changes recommended at this time.