OBJECTIVES

The objectives of this assessment are as follows:

- To enumerate the functional areas in the Information Services (IS) environment within which risk must be evaluated
- To provide a survey of risks in each of the functional areas
- To outline the mitigation strategies put in place by Sample Bank
- To provide a coherent baseline from which to coordinate cross-functional risk identification and mitigation

APPROACH

This document is a contextual framework which outlines the high-level risks, related to technology functional areas, identified by the Bank, and the strategies used to mitigate them. Detailed documentation of the policies, procedures and standards which enable these mitigations will be referenced here but will not be included.

The assessment was constructed based on a collaborative effort between Information Services and Security personnel.

The assessment will cover the following functional areas:

1. Information Services
2. Technology Committee
3. Vendor Oversight
4. Network Administration and Security
5. Network Infrastructure and Topology
6. Business Continuity Planning
7. Physical Security and Environmental
8. Information Security (customer information and databases)
9. System Development Life Cycle
10. Change Control
11. Application Portfolio

FUNCTIONAL AREA ASSESSMENTS

1. Information Services

The Information Services (IS) organization is guided by a Technology Plan, based upon the Bank's Strategic Plan and approved by the Senior Management Team and the Board of Directors. This plan includes an assessment of relevant, available technology opportunities and the business outcomes expected as the proposed implementation strategies are followed. The plan also includes a tentative list of projects to be executed over the three-year planning horizon.

The IS management structure is designed to help ensure that IS adds value to the business and that IS risks are mitigated. The structure supports adequate segregation of duties and promotes the achievement of the organization's objectives by allowing the teams within IS to focus on their areas of responsibility while encouraging cross-team participation.

An ongoing risk in any Information Services department is turnover resulting in loss of needed skills and intellectual property. In the Bank's IS department, all key personnel have individuals who could step into the key role in the event of illness or attrition (including the Vice President of Information Services). Currently, Information Services has areas where certain skill sets are held by only one person. Management has identified these areas and mitigation strategies, such as contacting a knowledgeable vendor or providing additional training to other staff, are in place.

The Bank's IS staff engages in separation of duties with regard to application code and deployment issues. This separation is audited by internal and multiple external auditors.

2. Technology Committee

The successful execution of the three year technology plan is overseen by the Technology Committee.

The Technology Committee is also the point of entry into the Bank for new technology, new technology-related projects, and new technology vendors. Each of these is given a risk rating by the business owner of the system and these are presented to the Committee using the Risk Assessment Matrix form. The ratings and mitigation strategies are reviewed by the Committee before the new component is accepted into the environment.

All new technology is reviewed by the Technology Committee for architectural consistency, security, compliance, vendor alignment, risk, and cost/return.

Also, all vendors assessed as critical vendors are examined annually by the Technology Committee (see below).

3. Vendor Oversight

Applications, services, and vendors which have been rated as mission critical by the Technology Committee are reviewed on an annual basis and reported to the Board of Directors. The business owner of the vendor relationship is responsible for presenting the review and working with the Chair of the Technology Committee to coordinate IS resources to perform the technology review.

The vendors are reviewed for financial viability. Their financials and balance sheets are assessed (whether they are public or privately held), and their recent sales activity is documented as necessary.

Also reviewed are the product offerings of the vendors and the architectures the vendors are employing to evolve their products (e.g., how are the vendors implementing Service Oriented Architecture). The Technology Committee also reviews the distribution of the vendor's product(s). Those vendors with low distribution numbers are given additional scrutiny.

The Technology Committee also reviews the architectures the vendor is employing in their product(s) to ensure continuity and congruity with the Bank's architecture and Three Year Technology Plan.

4. Network Administration and Security

The primary network hardware platforms are Cisco (for routers, switches and firewalls) and Dell (for servers and desktops). The number of domain administrators is limited and logs of critical processes such as backups are produced and reviewed. Logs on critical servers in the production environment are sent to a log aggregation appliance which produces alerts when activities of interest occur. Windows authentication through Active Directory is role-based and administered through groups with specific permissions. Formal processes for changes in production network access rights are in place and require a review and approval by the applicable manager. Processes are also in place to delete accounts and access rights as personnel leave the Bank.

Firewall rules limit access to traffic and quarterly penetration testing verifies their effectiveness. External access for Bank personnel and vendors is limited to the use of a secure VPN encrypted with 3DES. An intrusion detection system is active on the network, but because the system is nearing end-of-life, training on the system is limited, and reports provided do not clearly indicate the severity of threats, it will be replaced by a system from SecureWorks which will provide better monitoring and reporting and constant updating to keep up with evolving threats. An intrusion prevention system is also active for core servers.

Desktop machines connected to the network comply with group policies which limit the granting of local administrator rights, enforce complex password standards, and limit the ability to install software. Desktop and server machines are protected by anti-virus software. Since policies do not allow indiscriminate downloading of unchecked software on most machines, the threat of 'spyware' is minimal. The complications which arise from peer-to-peer software such as Yahoo Instant Messenger are also mitigated in this way.

Operating system functionality and security patches are applied on a regular basis by an automated patch management system controlled by a network administrator. Patches are installed in a non-production environment before being applied to production.

The critical servers are monitored using the Microsoft Operations Manager software and alerts are sent to the appropriate support personnel.

The project list for 2008 through 2010 includes initiatives to improve network, application, and security monitoring and management, allowing the Bank to be more proactive in its problem resolution and prevention.

The electronic banking environment is based on the Fincentric iWealthview banking software and currently requires a user name / password combination for access. Embedded functions allow the customer to link to the third party bill pay provider site and to view check images online. Customers have the ability to transfer funds outside the Bank but the receiving account must be pre-registered and approved by Bank personnel. Multi-factor authentication will be provided as a part of the Bank's conversion to the ORCC Internet Banking platform coincidental with the core conversion.

5. Network Infrastructure and Topology

The Bank's internal network is protected behind firewalls and access requires traversing these firewalls or entry through secure leased circuits. Penetration testing is done quarterly and critical items found on network devices or servers are remediated immediately. The Bank uses an IP telephony system. The telephony traffic is limited and does not leave the Bank's secure network as IP traffic.

The Bank's network provides failover paths to each branch. The primary link is between a branch and the Admin site. In the event of a down primary circuit a secondary line allows the branch to remain active through our disaster recovery site where data is forwarded on to Admin.

The networks are monitored for performance. Tools purchased in 2007 have increased our ability to monitor the network and diagnose problems. Changes, other than normal maintenance, made to network devices are reviewed with the Design Team, approved by Change Management, and applied only after gaining Change Management approval.

6. Business Continuity Planning

An initial Business Impact Analysis was completed in 2004 and the Bank's Business Continuity Plan is revised yearly. A disaster recovery test is done once each year as a formally managed project. The business criticality and restore priority of each application is verified at that time and adjustments to the plan are made accordingly.

Copies of the Business Impact Analysis, the Business Continuity Plan, and the results of the latest Disaster Recovery test are available for inspection.

7. Physical Security and Environmental

A suitable physical environment is required to assure the integrity of the computer equipment, network and data. General access to the Information Services area is limited to business hours. After hours access is restricted by proximity card readers. Access to the server room is strictly controlled by proximity card and alarm systems. Personnel, other than Information Services personnel and authorized equipment maintenance vendors, who need to access equipment in the server area, are escorted at all times by Information Services staff. The server area is protected by a non-liquid (FM200) fire suppression system, an early warning (VESDA) fire detection system and is monitored for temperature and humidity variations. Wiring is channeled through overhead conduits, leaving the floor free of obstructions. All servers are connected to UPS systems and an external natural gas power generator to allow the Bank to maintain service, or to gracefully shut down service and switch to the disaster recovery facility if required.

8. Information Security

All personnel are accountable for compliance with legal and regulatory requirements.

Sample Bank Financial Group is a publicly traded company and, therefore, subject to Sarbanes-Oxley and Graham-Leach-Bliley Acts. IS staff is responsible for ensuring that documentation of controls remains current and complete. Responsibility for the development, implementation, and monitoring of the Bank's Information Security programs belongs to the Information Security Officer.

- Encrypted backups in 2007
- Backups stored off-site
- Administrator passwords are never blank
- DBAs are not domain admins
- Training on information security provided
- Auditing of access

9. Systems Development Life Cycle (SDLC)

A formal SDLC process has been in place since 2004. Enterprise projects initiated since then have been managed using this methodology. The methodology covers both in-house developed and vendor-delivered functionality and defines a project from initiation through implementation. The process was developed in partnership with Sogeti USA LLC and covers processes, changes in scope or deliverables, roles and responsibilities, documentation and compliance, and product delivery and review. The process has been audited by both internal audit and external regulators. Like most methodologies, it is in a state of evolution meant to match the Bank's level of need.

IS is finalizing the framework of a Release Management practice to be fitted into the SDLC to increase the transparency of the process used to decide which functionality is included in new software releases.

10. Change Control

Changes to the production environment are coordinated through the Change Management Committee (CMC) which is made up of IS and business unit representatives and meets weekly. The Chair of the CMC reports process-related issues to the Technology Committee.

Notes documenting decisions of the CMC are published after each meeting for dissemination to key Bank staff and management.

All software and infrastructural changes implemented in the production environment are reviewed by the CMC for completion, assessment of efficiency, and customer impact.

11. Application Portfolio

The Fincentric, now Open Solutions, WB core processing applications, and the suite of applications surrounding them, including Portrait, Synergy, WES, and GECS, have had a history of poor performance and instability. The Portrait software was upgraded to a more stable release in 2007 and the 3.6.8 Fincentric service pack improved core stability and allowed us to upgrade GECS to a more current release.

Some of the Bank's systems lack components of the monitoring, auditing, and reporting functionality required for best-practices operation in the current environment. The Bank has worked with the application vendor, where possible, to ensure this functionality is included in future releases. When this has not proven effective, the Bank has built processes to extract the necessary data from the source system, or added manual controls around the associated business process.

The 2008 – 2010 Technology Plan calls for the conversion of the core system to the Harland Financial Solutions Phoenix system, a more stable, reliable, and industry standard platform. Ancillary systems such as Guthrie-Philips, APPRO, and FICS will also be converted to Harland products, reducing operational complexity and easing integration.

EVALUATION CRITERIA

Financial Risk – the impact the technology could have on the Bank's financial performance.

Operational Risk – the impact the technology could have on the Bank's effectiveness and efficiency.

Reputation Risk – the impact the technology would have on the Bank's ability to deliver appropriate customer service or secure customer data.

Transaction Risk – the impact that the incorrect processing of transaction would have on the Bank's ability to account for funds.

Strategic Risk – the impact the technology could have on the Bank's ability to achieve its strategic goals.

Regulatory Risk – the impact the technology could have on the Bank's ability to satisfy regulatory requirements.

Risks will be rated on the impact the technology may have on the Bank, not necessarily on the Bank's current position once all mitigating factors are take into consideration. Mitigation strategies in place or planned for will be discussed below. Risks will be rated on a scale of 1 (low risk) to 5 (high risk). Combined totals in the range of 1 – 12 are considered low risks. Totals between 12 and 22 are medium risks. Any total above 23 is considered high risk.

RISK MATRIX

IT Risk Factors >>>	FINANCIAL RISK	OPERATIONAL RISK	REPUTATION RISK	TRANSACTIONAL RISK	STRATEGIC RISK	REGULATORY RISK	Combined Risk Rating
IT Risk Entities							
Information Services	2	3	3	3	1	3	15
Technology Committee	2	2	2	1	5	2	14
Vendor Oversight	3	3	3	1	3	3	16
Network Administration and Security	3	4	4	4	2	4	21
Business Continuity	3	2	2	3	2	2	14
Network Infrastructure and Topology	2	5	5	2	3	4	21
Information Security	5	5	5	5	4	5	29
Physical Security and Environment	2	4	4	2	2	4	18
Change Control	3	5	4	2	4	5	21
Application Portfolio	5	5	5	5	5	3	28
Project Management & SDLC	3	3	2	2	5	4	19

RISK SUMMARY

The Bank has 2 areas of significant risk:

Information Security
Application Portfolio

Mitigations in Place or Planned

Information Security: The Bank is replacing a large portion of out-of-date network equipment in 2008 and addition replacements are scheduled for 2009. The Bank has contracted for third party intrusion detection and other monitoring from an industry leading vendor. Additional network

segmentation and isolation of the database servers will be planned along with the infrastructure component project of the core banking system conversion in 2009. Critical Human Resources and Accounting network shares will be moved to more easily secured locations. The Active Directory upgrade planned in 2008 will also provide better security and better reporting capabilities than the current version.

Application Portfolio: The Bank has an application portfolio containing systems which are complex to operate and contain components which are not in the mainstream of information technology. The integration of these disparate systems adds to the environmental complexity. The Bank has an active strategy to convert many of these systems to products in line with our new core system in 2009. Many of these components were upgraded in 2007 to more stable and reliable versions and the Bank has begun to de-couple reporting from these systems onto an internal Reporting Services platform which will allow for better data integration and the production of reports not produced in the current systems.

The Bank is actively working with vendors to increase security on application platforms. For example, based on the architectural review, several changes were requested of, and obtained from, the Branch Capture vendor in order to bring the SQL Server and the application server up to the standard Sample Bank security configurations.