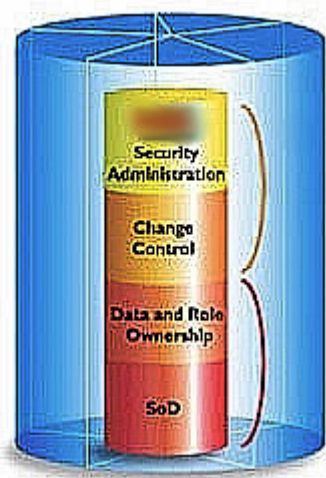


LEWIS UNIVERSITY
68-595 MSIS INFORMATION SECURITY
CAPSTONE PROJECT



GLOBAL MARKETS

OPTI MANAGEMENT RESOURCES (OMR)

SEGREGATION OF DUTIES

STUDENT:

ALBERT STANLEY

PROFESSOR:

JOSEPH N.V. NINH

PROGRAM DIRECTOR:

RAY KLUMP, Ph.D

SUMMARY

Project Goals & Objective

The objective of this project is to segregate the duties and responsibilities of the Opti Management Resources (OMR) trading application used in all 62 countries, which would eliminate conflicts base on Sarbanes Oxley Act (SOXA) conflict definitions.

Group Audit along with E&Y representing Sarbanes Oxley (SOX) performed an audit of logical security and automated controls for the Opti Management Resources (OMR) application. The specific scope included testing of significant automated controls, reviewing the application security architecture and evaluating security administration over the applications, data and program files.

Background and control environment

The Opti Management Resources (OMR) application is the booking system of record (both Front and Back Offices) for the on-balance sheet deposit and loan activities comprising the Banking & Funding books for the Foreign Exchange & Money Markets businesses based in Chicago. All trade processing for the Chicago Treasury Foreign Exchange Operations and Chicago Treasury Money Market Operations are recorded in the Opti Management Resources (OMR) system. The Opti Management Resources (OMR) production application server is managed by an external vendor, SS&C Technologies, Inc. OMR Systems International Limited, and resides on a Mainframe/VMS environment which is hosted by ADP in New Jersey. The Sybase

production database runs on a Unix server located in Chicago at the ABN AMRO Plaza at 540 W. Madison.

Phase 1 Process

To accomplish the project's goal, I'll have to obtain:

- A system generated listing of all users including user ID, Name, Profile (group/type), Access privileges and rights
- An access Request/Approval Documentation (Sample selection will be provided)
- A distribution list for periodic review of access privileges.
- Terminated Employee Reports from H/R (at least 2 versions).

Phase 2 Process

After acquiring the materials identified in Phase 1, I performed the following tasks:

- Run "Conflict Report" based on system generated user listing gathered in phase 1.
- Meet with senior management and department heads to go over results from "Conflict report".
- Establish a suitable solution to eliminate and/or mitigate "Conflicts" generated from report. Then rerun "Conflict Report".

TABLE OF CONTENTS

Sections

Introduction to ABN AMRO	7
<ul style="list-style-type: none">• How ABN AMRO came to be• ABN AMRO in North America	
Introduction to Segregation of Duties (SoD) Project	12
<ul style="list-style-type: none">• User ID Structure• User Access Hierarchy• Process for granting view only rights• Process for Mapping Transactions to Users• SOXa Issues	
What is Segregation of Duties?	14
What is Sarbanes Oxley (SOX)?	16
<ul style="list-style-type: none">• The Buck Stops with IT• What is the Sarbanes-Oxley Act (SOXA)?	
Procedure	23
<ul style="list-style-type: none">• Description of Application• Business Components• Information Technology Component	
Report details	26
<ul style="list-style-type: none">• An Overview of the Top Down Approach• Internal Control Deficiencies• Logical Security Control<ul style="list-style-type: none">1. Periodic Access Reviews2. User Account Removal	
Conclusion	38
<ul style="list-style-type: none">• On the Business Side• On the Information Technology Side	
Appendices	44
References	49

LIST OF TABLES

Table 1: Sample of Id Structure before project Started	23
Table 2: Sample of suggested Id Structure Changes	32
Table 3: Sample of Id Structure after project Changes	33

INTRODUCTION TO ABN AMRO

The history of ABN AMRO spans more than 175 years. From a trading society chartered under King William I ABN AMRO has grown and evolved to its modern Strategic Business Unit structure. This growth has occurred in North America, and around the world. Today we are able to focus on the specific and increasingly sophisticated needs of our customers while offering a complete array of solutions to meet the complete scope of their financial needs.

How ABN AMRO's came to be?

Algemene Bank Nederland (ABN)

ABN AMRO traces its roots to 1824, when King William I of The Netherlands issued a Royal Decree to establish Nederlandsche Handel-Maatschappij (Netherlands Trading Society) in Amsterdam. By this point in history, Amsterdam had already assumed a role as a key European financial and banking center. The king and the company's founders set up the Netherlands Trading Society to expand trade relations and open new commerce channels. This early outreach extended to China, Singapore and the Dutch East Indies (Indonesia). Changes in the financial structure of the Dutch East Indies motivated the Netherlands Trading Society to turn its attention to banking. Business such as credits, time deposits and security orders sustained the bank in the late 1800s. After World War II, the bank focused on expanding its network by opening branches throughout the Netherlands and abroad. In October 1964, Nederlandsche Handel-Maatschappij and De

Twentsche Bank merged to become Algemene Bank Nederland (ABN), the Amalgamated Banks of The Netherlands.

ABN continued its growth and expansion with the December 1967 takeover of Hollandsche Bank-Unie. Because of Hollandsche Bank-Unie's strong presence in South America, ABN now achieved a more balanced international network.

In June 1972 ABN Corporation came into existence, representing ABN's subsidiaries in the United States.

In the late 1970s, acquisition of LaSalle National Bank (LNB) in Chicago brought ABN firmly into the U.S. Midwest. In 1979, LaSalle ranked as the sixth largest bank in Chicago and had 700 employees. In 1986, ABN Company, Inc. took over management of all ABN offices and affiliates in the U.S. and Canada and the name ABN Company, Inc. was changed to ABN/LaSalle North America, Inc.[\[6\]](#)

■ Amsterdam-Rotterdam Bank (AMRO)

A rivalry between the Dutch cities of Rotterdam and Amsterdam had existed for hundreds of years. As Amsterdam's commerce and culture flourished, Rotterdam closely followed. The city of Rotterdam also plays a substantial role in ABN AMRO's history. This part of the history begins with the creation of the Rotterdamsche Bank in 1863 by a group of businessmen and bankers. Styled after Britain's Colonial Bank, Rotterdamsche Bank lent funds to companies operating in the Dutch East Indies. Eventually, this bank localized its lending activities in the Netherlands and began looking at expanding into the securities business. In the early part of this century, several mergers added brokerage and securities capacities to the firm, as well as securing coveted entry into the Amsterdam

Stock Exchange. In quick succession, the new bank - named the Rotterdamsche Bankvereeniging or Robaver - acquired numerous local banks. By the early 1920s, Robaver became one of the largest banks in the Netherlands. While Robaver accumulated smaller banks, it also established overseas banks, including those in the West Indies and Russia. Always a forward-thinking company, Robaver established Vrouwenbank, a bank specifically for women in 1928.

In this continuing story of mergers, a major player was the Amsterdamsche Bank. This bank was established in 1871 to serve as an instrument in bonding the Dutch and German money markets. After continued expansion, Amsterdamsche Bank began a period of consolidation. In 1964, Amsterdamsche Bank and Robaver merged to become the Amsterdam-Rotterdam Bank (AMRO).

In 1968, AMRO, Deutsche Bank of Germany, Société Générale de Banque of Belgium and Great Britain's Midland Bank became shareholders in the European American Bank and Trust Company in New York. AMRO continued power-building by increasing its retail banking business during the 1960s and 1970s. [\[6\]](#)

■ Creating ABN AMRO

With European unification becoming a reality in the early 1990s, ABN and AMRO announced in March, 1990 that they were considering a merger. On September 22, 1991, the merger of ABN and AMRO was consummated and the articles of association amended to create ABN AMRO Bank N.V.

To facilitate the integration of the disparate but complementary pieces of the

new organization, ABN AMRO's core values message was created. The ABN AMRO Bank Board of Directors selected the four Core Corporate Values - integrity, respect, teamwork and professionalism - to represent the organization's working values. [\[6\]](#)

ABN AMRO in North America

During the 1970s, ABN had acquired and grown LaSalle National Bank. During the late 1980s LaSalle National Bank acquired Lane Financial, Inc. and Exchange Bancorp, Inc. In October 1990, anticipating the merger between ABN and AMRO, ABN/LaSalle North America, Inc. was changed to ABN AMRO North America, Inc.

From 1991 to the present, ABN AMRO has continued to acquire financial institutions in North America. The result is LaSalle Bank Corporation is now one of the largest banking companies in the US and one of the largest foreign-owned banks in the country.

The 1997 agreement reached to acquire Standard Federal Bancorporation brought Standard Federal Bank (SFB) and its Michigan-based InterFirst and Chicago-based Bell Federal Bank divisions into the ABN AMRO fold. In 2000, ABN AMRO purchased Michigan National Corporation and its Michigan National Bank subsidiary. Merging this bank with Standard Federal Bank created the second largest bank in Michigan, with the critical mass to operate in both the retail and commercial sector. Standard Federal Bank is one of the Midwest's leading home mortgage lenders and operates a network of more than 150 banking centers, and commercial banking offices, including 12 home-lending centers, in Michigan and Indiana. The acquisition reinforces ABN AMRO's position as one of the largest foreign commercial bank in the US.

Also in 1997, ABN AMRO Bank's international network was further expanded with the bank's listing of its shares on the New York Stock Exchange (ABN:NYSE). In the same year, ABN AMRO and ABN AMRO Chicago Corporation (name later changed to ABN AMRO Incorporated) reached an agreement with Citicorp to take over its futures activities.

In 2000, ABN AMRO purchased the New York business of ING Barings, an investment bank and bought Allegheny Asset Management.

This North American expansion provided ABN AMRO with the strength and depth to operate in each of the banks key business units when the bank announced its strategic realignment in 2000.

INTRODUCTION TO SEGREGATION OF DUTIES PROJECT

This ABN AMRO Segregation of Duties project gives us an understanding of application security for the Opti Management Resources (OMR) application.

Specifically, the segregation of duties developed in this work addresses the following:

a. User ID Structure: Individual users in Opti Management Resources (OMR) are assigned a unique user ID for every functional template or instance of a template they have access to (see below for discussion of functional templates). Many Opti Management Resources (OMR) users have multiple IDs assigned the same template to facilitate processing more than one transaction in the environment at the same time (i.e., one entry per User ID).

b. User Access Hierarchy: There are two high levels of access that are assigned to a user in Opti Management Resources (OMR):

1. Functional Template – Screens and transactions a user has access to.
2. Organizational Template – The region / set of books that a user has access to for each specific functional template.

Individual rights within a specific functional template cannot be limited or altered.

c. Process for granting view only rights: While individual transactions within a template may be view-only, the only functional template which gives a client completely

view-only access is the INQ (inquiry) template. This functional template will not limit any functionality granted to users in other templates they have been assigned.

d. Process for Mapping Transactions to Users: Application security was provided in roughly 30 text files (one for each template). The functional templates are laid out by function levels: Level 1 functions are always the first non-indented line (and represent the highest level activities); Level 2 functions are the second non-indented line and represent a more granular set of activities; Level 3 are transactions associated with the first and second level functions.

To understand a user's full functionality, the user list is mapped to the OMR application security data by the functional template. See **Table 3** on page 35.

e. SOXa Issues: In some instances, the same user has multiple OMR IDs with trade/data entry access, this allows this user to enter a trade and also release/approve it.

To solve this issue, the following (see example below) was adopted. A sample of these changes can be seen in Table 3.

Example:

1st OMR ID - No change in ID name, application access, and password.

2nd OMR ID - Change the application access to inquiry only

3rd OMR - if applicable should be deleted.

WHAT IS SEGREGATION OF DUTIES (SOD)?

Segregation of duties splits the responsibility of a critical task among different people.

The method has always been needed to provide checks and balances against fraud or error, but in many companies, separation of duties has not been fully implemented and practiced. Many auditors, however, will be looking for this control technique when testing for compliance. [\[8\]](#)

You ask about separating access to development and production environment software and its components. Software developers should not have access to software components that are running in a production environment, since keeping limited access prevents potential fraudulent activities and ensures the availability and stability of the environment. If software developers need to tweak some software component that is in a live production environment, they -- like everyone else -- should follow a change control process. Such a procedure evaluates the problem, calculates implementation costs, designs a fix and reviews the fix's ramifications; examples would be if the fix causes interoperability issues with other software, if it opens a new vulnerability or if it negatively affects availability. The fix is then built on development (not production) systems, and then tested by another person or group in charge of quality assurance. After the fix is documented, the software version is increased to demonstrate its change, and then the fix is deployed. When working with in-house developers, have them save their

code to a database that carries out version control, and back it up either each day or each week. [\[9\]](#)

Organizations cannot implement separation of duties without establishing logical controls. Every organization should be able to configure their access controls to allow authorized individuals to access the necessary resources. This can be done at the domain level, resource level, and file and directory level. If an organization cannot purchase a software package that specifically provides a separation of duties functionality, then they'll need to implement tight access control with strict individual accountability and thorough management supervision.

It's easier to implement separation of duties if solely attempting to ensure that developers do not interact with production code and operational employees do not interact with development code. In this case, simply configure the access control lists on the different libraries and set which operations each user or group can carry out. You can also implement an automated configuration management tool like Tripwire to detect any changes in production code. It's also worth noting that it's much more difficult to implement separation of duties when you have to split up actual transaction steps or business processes that take place across more than one application or system. Because of the complexity that is involved with these more intrinsic activities, there are products that automate such implementations. They allow the administrator to set the rules through a rule engine and enforce them when a user tries to carry out various operations.

WHAT IS SARBANES-OXLEY (SOX)?

Sarbanes-Oxley (SOX) is part of the new business reality for U.S. public corporations. Ongoing compliance is essential to maintaining shareholder confidence and avoiding penalties making SOX the most important corporate governance and disclosure legislation since the U.S. security laws of the 1930s.

Section 404, which stipulates company management must demonstrate control over financial reporting, is arguably the most significant part of the legislation -- affecting companies with year-ends beginning on or after November 15, 2004. [\[12\]](#)

Of particular concern to IT is one of the four IT General Control objectives specified by the U.S. Public Company Accounting Oversight Board (PCAOB), Access to Programs and Data.

The Buck Stops with IT

Today, a company's financial reports summarize processes supported by enterprise systems and applications running on sophisticated servers databases and networks. IT processes and controls that are integral to that framework need to satisfy the broader requirements of SOX.

However, many IT organizations lack these controls and most do not have the means to document them or their effectiveness on an ongoing basis.

For some companies, documenting existing processes may be adequate to pass the initial audit. For most publicly-held corporations, though, automated software systems will be required.

The intent of the SOX IT audit is to verify that processes and controls are in place and consistently followed. Manual, paper-based solutions are unlikely to be sufficient on an ongoing basis. In the case of large or geographically dispersed organizations, auditors generally probe more intensively for proof of adequate controls and consistently followed processes.

User access rights and procedures should be standardized and enforced. Compliance and controls can be automated with a self-service provisioning process. With an automated process, the appropriate employees are given access to the right applications and data; and when an employee's functional role or authorization changes, access to those systems is automatically and immediately adjusted.

This automation not only formalizes and ensures control over your application security processes, but it also generates a complete audit trail that demonstrates these processes were followed; a single source where application access and related controls can be tracked to monitor compliance.

Finally, it enables ongoing accountability and a framework to drive future information security and compliance initiatives.

Indeed, the requirements for internal controls continue beyond the initial Section 404 filing: IT organizations must prepare for future compliance after the first successful attestation and filing. Unlike previous event-driven control activities such as year 2000 (Y2K), SOX [\[13\]](#) has become part of doing business and IT will continue to have an important role in internal control over financial reporting. Organizations must develop an

ongoing compliance monitoring process, because the full impact of SOXA will not be known for several years.

What is the Sarbanes-Oxley Act (SOXA)?

Sarbanes-Oxley Act is a US law passed in 2002 to strengthen corporate governance and restore investor confidence [\[1\]](#). Act was sponsored by US Senator Paul Sarbanes and US Representative Michael Oxley. Legislation is wide ranging and establishes new or enhanced standards for all US public company Boards, Management, and public accounting firms. Sarbanes-Oxley law contains 11 titles, or sections, ranging from additional Corporate Board responsibilities to criminal penalties. Requires Security and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law. The Sarbanes-Oxley Act makes corporate executives explicitly responsible for establishing, evaluating and monitoring the effectiveness of internal control over financial reporting.

While Sarbanes-Oxley is financial legislation, at its heart it is about ensuring that internal controls or rules are in place to govern the creation and documentation of information in financial statements[\[2\]](#).

Based on SOX Sections 302 and 404 management is forced to take a more serious interest in the internal controls of the bank

SOX Section 302 - Corporate Responsibility for Financial Reports [\[3\]](#)

- a) CEO and CFO must review all financial reports.
- b) Financial report does not contain any misrepresentations.

- c) Information in the financial report is "fairly presented".
- d) CEO and CFO are responsible for the internal accounting controls.
- e) CEO and CFO must report any deficiencies in internal accounting controls, or any fraud involving the management of the audit committee.
- f) CEO and CFO must indicate any material changes in internal accounting controls.

SOX Section 404: Management Assessment of Internal Controls

All annual financial reports must include an Internal Control Report stating that management is responsible for an "adequate" internal control structure, and an assessment by management of the effectiveness of the control structure [4]. Any shortcomings in these controls must also be reported. In addition, registered external auditors must attest to the accuracy of the company management's assertion that internal accounting controls are in place, operational and effective.

Legislators in virtually every nation have promulgated laws that mandate higher levels of corporate governance, risk management, and compliance. [7] From the Sarbanes-Oxley Act (SOXA) in the U.S., to Bill 198 in Canada, to Japan's Financial Instruments and Exchange Law (the so-called J-SOX), the current regulatory environment worldwide is one that demands enterprises take every step to ensure the integrity of their finances, data, processes, and employees. Central to this is the need to control access to corporate information, functions, and processes, and to ensure that there is comprehensive Segregation of Duties (SoD) across the entire enterprise and at all levels of corporate functioning.

Unfortunately, for many companies the cost in money and resources to ensure compliance with access control, Segregation of Duties (SoD), and compliant user provisioning on an ongoing basis can be overwhelming. In fact, for companies that have a multitude of software solutions and applications, this task may seem to be virtually impossible. Establishing and maintaining a comprehensive and consistent library of Segregation of Duties (SoD) policies and rules, provisioning new and transferred employees, and adding new rules as functions, duties, and responsibilities change are difficult challenges for any enterprise. Even companies that have deployed access control or risk management solutions find it can be extremely difficult to translate the business definition of a particular risk into a technical definition of that risk that the solution will understand. To address these key business challenges and ensure SOX compliance consistently year after year in a sustainable fashion, forward-looking companies are seeking enterprise-ready GRC solutions.

From the perspective of an executive and business process owner, an enterprise-ready solution must empower employees to do the right things, while enforcing things are done right. The solution must enforce accountability and enable transparency so that business owners and executives can ultimately sign-off on their attestations with confidence. As a result, compliance issues such as access control, proper segregation of duties (SoD), and compliant provisioning must be managed by a solution that should span all core business processes and across all enterprise application software. A central policy repository can then ensure consistency across the enterprise. [\[10\]](#)

From an IT perspective, this enterprise-readiness translates into a number of requirements.

First and foremost, IT managers want an application delivered with a pre-defined best practice library of comprehensive cross-process and cross-application policies. On one hand, this vast number of policy rules must be easy to enhance and to adjust as the business changes. On the other hand, rules must be granular enough to address all of the details of enterprise application software, catching all the violations without producing false positives.

Second, the solution must empower employees across the enterprise. Efficient and effective collaboration between business and IT is one of the keys to success here. Automation and dynamic workflow options not only ensure reliability and repeatability of the solution by avoiding manual errors and establishing institutional knowledge, they also accelerate processes and increase efficiency.

Third, the solution must be able to demonstrate compliance across the enterprise. It must maintain auditable records that internal and external auditors as well as regulators can use to verify compliance. Some relevant audit questions in the access control area include: Who has access to a given system? What authorizations do they have? Who granted access and when? Was it properly approved? [\[11\]](#)

Fourth, to satisfy the needs of the IT department, the solution must have scalable, robust, and open software architecture, and be a solution that fits into any given IT system landscape. The solution should provide a range of extensibility options to meet unique business process or IT requirements.

PROCEDURE

The procedure to accomplish our goal would be done through a long term Segregation of Duties (Separation of Duties) “Work Streams” components. These work stream components would be most effective if the approach was to concentrate in the following two areas of the organization. The areas are Business and Information Technology. First, let’s get a better understanding of the application.

Description of Application:

OMR Systems Corporation and OMR Systems International Limited (collectively “OMR”), previously a division of Automatic Data Processing-Brokerage Services Group (ADP-BSG), was acquired by SS&C Technologies, Inc. on April 12, 2004. Opti Management Resources (OMR) provides automated trade and back-office funds processing solutions for the global financial services industry.

Opti Management Resources (OMR) Trading Assistant (TA) is a comprehensive trading system from OMR that handles Forex, Money Market, Securities, Derivatives and bullion transactions from one trade entry screen. The processing incorporates trade validation, advice/payment processing, accounting, online positions, cash flows and risk management. TA is a fully automated, scalable straight-through processing solution that handles all trade processing, as well as portfolio and risk functions across all products, currencies, instruments and locations.

Business Components:

- a. Finalize Segregation of Duties (Separation of Duties) approach.
- b. Design Segregation of Duties (Separation of Duties) Roles & Responsibilities and Supporting Processes.
- c. Execute Segregation of Duties (Separation of Duties) Processes.
- d. Define business conflicts.
- e. Define Application and Enterprise Roles.
- f. Transition users to Segregation of Duties (Separation of Duties) business model

Information Technology Components:

- a. Build reporting infrastructure.
- b. Deploy reporting infrastructure.
- c. Enhance Conflict Management Tool.
- d. Deploy Segregation of Duties (Separation of Duties) Conflict Management Tool.
- e. Integrate additional applications

The necessary information needed was gathered as follows in two sets:

Below is the set 1 information:

- a. A listing was generated of all users including user ID, Name, Profile (group/type), Access privileges and rights. A sample of this can be seen in Table 1. This gives us the visual evidence of the id structure in place and also indicates the number of conflicts we need to fix.

- b. The Access Request/Approval Documentation, this document saves us a lot of time as to which managers needs to be contacted and draft into the process.
- c. A copy of the distribution list used for periodic review of access privileges.

Below are the set 2 information:

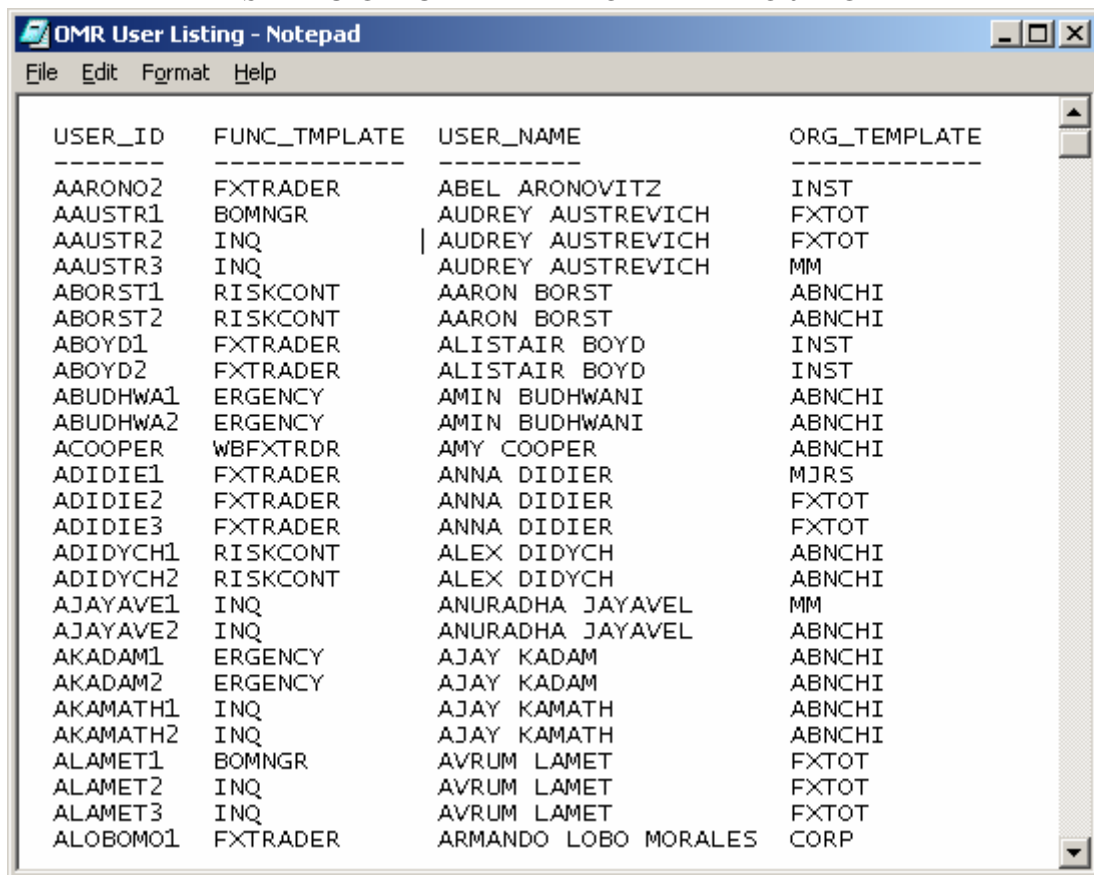
- a. Run “Conflict Report” (**See Appendix A**) based on the user listing generated in set 1. In this report, section A. ‘General File Count’ shows the raw data for total number of users who has access to this application, total number of security functions this application supports and total number of user transactions mapped to the analysis tool/software.

In section B. “User Specific Count’ section spelled out some of the unique accounts or accounts with unique functions. While section C. ‘Conflict Counts’ was a little more detailed in that, it highlighted the number of conflicts, number of users with conflicts etc.
- b. Meet with senior management and department heads to go over results of reports.
- c. Establish a suitable solution for the continuous rerunning of the “Conflict Report” until all “Conflicts” have been eliminated and/or mitigated.

REPORT DETAILS

The Sarbanes-Oxley Act has heightened awareness of the need for more robust internal controls and increased financial statement scrutiny. As a result, ABN AMRO's senior management requested and received copies of the user listing report, an example of which is shown in **Table 1**.

TABLE 1
ID STRUCTURE BEFORE PROJECT



USER_ID	FUNC_TMPLATE	USER_NAME	ORG_TEMPLATE
AARON02	FXTRADER	ABEL ARONOVITZ	INST
AAUSTR1	BOMNGR	AUDREY AUSTREVICH	FXTOT
AAUSTR2	INQ	AUDREY AUSTREVICH	FXTOT
AAUSTR3	INQ	AUDREY AUSTREVICH	MM
ABORST1	RISKCONT	AARON BORST	ABNCHI
ABORST2	RISKCONT	AARON BORST	ABNCHI
ABOYD1	FXTRADER	ALISTAIR BOYD	INST
ABOYD2	FXTRADER	ALISTAIR BOYD	INST
ABUDHWA1	ERGENCY	AMIN BUDHWANI	ABNCHI
ABUDHWA2	ERGENCY	AMIN BUDHWANI	ABNCHI
ACOOOPER	WBFXTRDR	AMY COOPER	ABNCHI
ADIDIE1	FXTRADER	ANNA DIDIER	MJRS
ADIDIE2	FXTRADER	ANNA DIDIER	FXTOT
ADIDIE3	FXTRADER	ANNA DIDIER	FXTOT
ADIDYCH1	RISKCONT	ALEX DIDYCH	ABNCHI
ADIDYCH2	RISKCONT	ALEX DIDYCH	ABNCHI
AJAYAVE1	INQ	ANURADHA JAYAVEL	MM
AJAYAVE2	INQ	ANURADHA JAYAVEL	ABNCHI
AKADAM1	ERGENCY	AJAY KADAM	ABNCHI
AKADAM2	ERGENCY	AJAY KADAM	ABNCHI
AKAMATH1	INQ	AJAY KAMATH	ABNCHI
AKAMATH2	INQ	AJAY KAMATH	ABNCHI
ALAMET1	BOMNGR	AVRUM LAMET	FXTOT
ALAMET2	INQ	AVRUM LAMET	FXTOT
ALAMET3	INQ	AVRUM LAMET	FXTOT
ALOBOMO1	FXTRADER	ARMANDO LOBO MORALES	CORP

A meeting was called between the business and IT units to determine the best way to fix and mitigate the various issues, if any existed. From this meeting it was established there has to be tighter information technology controls specific to financial application system

access and authorization privileges. The main area which needed immediate attention was the lack of centralized control over user administration processes. For instance, a person leaves the bank or changes job responsibilities, security and access control issues became evident because:

- a. Lack of a centralized automated mechanism of communicating to the various account administrators, that the user access should be terminated or changed.
- b. Lack of administrative controls to ensure the various departments like Human Resources, Help Desk, IT Administrators are completing the necessary steps.

Also from his meeting management was able to evaluate the process, transaction, and application level-controls, which provided a good deal of the evidence, which they needed to support an overall assessment of the effectiveness of internal control over financial reporting. This led them to consider controls, including information technology (IT) controls, which serve to prevent or detect errors of importance relating to each significant account.

A wealth of information came from the meeting because management was able to consider controls that address each of the five components of internal control:

- Control Environment
- Risk Assessment
- Information and Communication
- Control Activities
- Monitoring

Controls relating to several of these components control environment, risk assessment, and monitoring often are at a higher level and must be evaluated carefully to determine whether the controls are sensitive enough to prevent or detect errors of importance or fraud relating to each significant account [\[17\]](#). Many of the more detailed controls that management will identify to support its assessment will be from the information and communication and/or control activities components and primarily relate to specific processes and applications.

Additionally, ABN has been subject to external and internal audits regarding access privileges and segregation of duties that have resulted in management letters of audit findings. A conflict analysis report was run. The deliverable presented in **Appendix B** is the initial results of the Separation of Duties conflict analysis. Samples of the transactions were mapped to activities on the conflict matrix (**Appendix C**) for closer analysis. A message was left with the folks from Deloitte requesting their assistance in pushing us across the finish line with this project from a Segregation of Duties/conflict perspective plus providing future guidance on our SOXA ambitions. It was also concluded we need to leverage this experience for our end state model and also support the extensive work and effort that has been invested to date.

The initial meeting with the folks from Deloitte was to have them provide us with a walk-through of the current process / methodology being used to gather the information mentioned in Set 1 which will be used to form the going forward tool. It was also determined that we needed to make sure the rollout document and procedures to be

developed will serve all of our respective purposes. So, it was decided the 'Top Down Approach' was the best way to precede.

An Overview of the Top Down Approach

This approach is methodical, more precise, but can be slow and have high initial costs.

Where security needs to be "urgently" improved, the top down approach has been known to have a long term, precise policy, strategy and vision on security that is supported and understood by management.

The top down approach involves: [14]

1. Asset Analysis: What needs to be protected? List information and processes (What are the important assets? Are they stored on computer? What are the financial implications of loss of these assets?). The measures taken to protect assets should correspond to the value of assets.
2. Analyse current security rules/policies/practices (if any).
3. Define basic Security Objectives: e.g. fix basic Availability, Confidentiality and Integrity objectives.
4. Threat Analysis: Before deciding how to protect a system, it is necessary to know what the system is to be protected against i.e. what threats are to be countered. Identify Threats (employee vengeance, hackers, espionage, technical failures etc.). A list of sample threats is presented later. Threats tend to be general in nature.

5. Impact Analysis:

- What is the impact or consequence (harm to business) if a threat, or a combination of threats is realised? This is very system specific, e.g. loss of company secrets, modification of accounting data, falsification of money transfers.
- The impact should be judged by business experts, not technical experts.
- The impact has two components, a short term impact (threat is short) and a long term impact (the threat persists, affecting the business in the long term). The total impact should be considered as a number (0-5) with a contribution for the short term and the long term.
 - a. The impact is negligible
 - b. The effect is minor, major business operations are not affected.
 - c. Business operations are unavailable for a certain amount of time, revenue is lost, customer confidence is affected minimally (unlikely to lose customers).
 - d. Significant loss to business operations or customer confidence or market share. Customers will be lost.
 - e. The effect is disastrous, but the company can survive, at a significant cost.
 - f. The effect is catastrophic, the company cannot survive.

As the project picked up momentum while using this approach, we found some obvious internal control deficiencies.

Internal Control Deficiencies

The following deficiencies were noted:

Adding/Modifying User Accounts - Out of a sample of 25 new and modified users, access requests for two new contractors did not have the secondary approval of the ABN application owner (Note: An additional 2 users sampled showed that secondary approval was provided for an application other than OMR. The assumption that this approval was implicit for all of the platforms for which access was requested on the form should have been verified and documented by the Security Administrator before access was granted). Additionally, one of 25 users sampled did not have sufficient evidence for a change in the user's account. The user's functional template was changed from "INQ" to "BOMNGR," an increase in system privileges. This is referred to as a 'Design Deficiency'.

Mid- term Action:

1. Update the user request form to reduce confusion
2. Provide EDS Security Administrator with a list of ABN AMRO authorities who can sign off for application user access. This list should be approved by the application owner.
3. Periodic review should be conducted to ensure the procedure is being followed.

Long term Action:

- a. Research and Utilize a more robust approval user access request process - TRM RAPTOR Project
- b. User Account Removal - an OMR User left the bank, but his User ID remained active with FX Trader permissions. Additionally, several active User IDs have FX Pay template permissions although this access is no longer necessary.

Immediate Action - continue to perform the quarterly user access review, and adding a step to the new procedure to request EDS to provide proof/ response / documentation for the user account removal. This is referred to as a 'Significant Deficiency'.

Long-term Action: Implementation of the TRM RAPTOR project

- c. Periodic User (Access) Review - OMR user reports distributed to managers to perform the quarterly review for the appropriateness of user access is not system generated. Manually updating listings of users creates a risk that human errors could be made.

Long-term Action:

- (1) Locate the proper system report within OMR application to fulfill the requirements
- (2) Update the procedure with the appropriate OMR report names so that it can be done repeatedly and correctly.

- d. Periodic User (Profile) Review - OMR user profiles (ie. functional templates) are not specifically assigned to owners who would be responsible for periodically reviewing access rights. (Issues also noted in SarbOx Control #09020101)

Long-term Action:

- 1) Locate the proper system report within OMR application to fulfill the requirements

- 2) Update the procedure with the appropriate OMR report names so that it can be done repeatedly and correctly.
- 3) Work with business to create the review process and ownership (part of Segregation of duties project)

Based on these deficiencies, the following control descriptions were agreed upon:

1. Security administration procedures provide guidance on how to properly manage security administration and establish a standard to ensure that proper controls are adhered to on a consistent basis. Detailed processes for user setup, modification, and deletion exist and are consistently performed by the application security administrators.
2. Setup of user access is initiated by a properly approved user request form.

Deletions and modification of user access rights are identified through prompt management notification, review of Human Resource reports, expiration dates on consultant and outside vendor IDs and/or disabling IDs after a period of inactivity. Reports are periodically provided to user management to validate access granted, and action is taken based on management's response.

The risk of granting unauthorized system access is normally mitigated by an effective periodic user access and user profile review. However, as noted herein, the periodic review process introduces deviations that create risk for failing to provide management with complete and accurate listings of users to review for appropriateness (and no

opportunity to review the permissions assigned to users). This risk would normally be mitigated by an effective process for adding and removing users from the system.

However, there are likewise, deviations in the process of adding new users. Moreover, Group Audit's testing for the appropriateness of user access showed that out of 25 users tested, one user had left the bank, but was not removed from the application.

Additionally, three user ID's remain from a separate interfacing system that was previously disconnected. (Also noted in SarbOx Control #09020101)

The Conflicts report results were captured in **Appendix A**.

A sample of some of the changes deriving from those reports can be viewed in **Table 2**.

TABLE 2

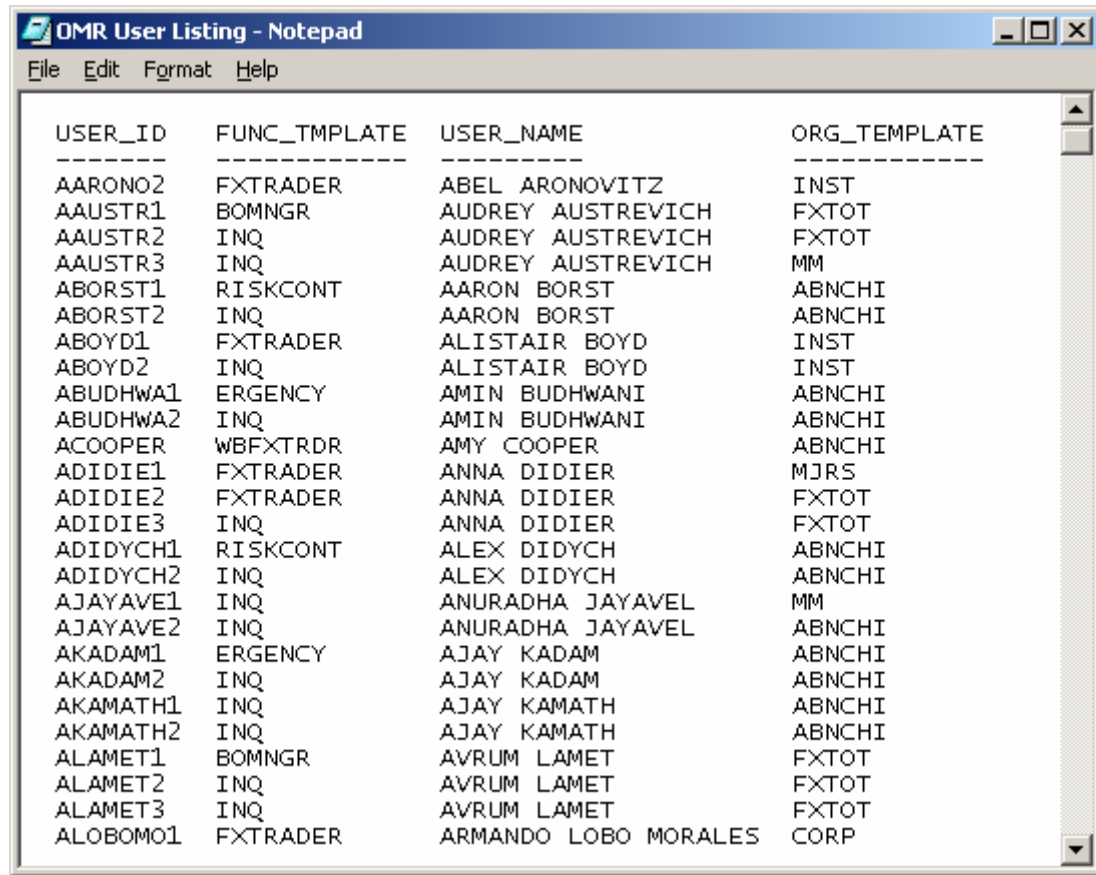
ID STRUCTURE CHANGES

USER_ID	FUNC_TMPLATE	USER_NAME	ORG_TEMPLATE	COMMENTS
AARONO2	FXTRADER	ABEL ARONOVITZ	INST	
AAUSTR1	BOMNGR	AUDREY AUSTREVICH	FXTOT	
AAUSTR2	INQ	AUDREY AUSTREVICH	FXTOT	
AAUSTR3	INQ	AUDREY AUSTREVICH	MM	
ABORST1	RISKCONT	AARON BORST	ABNCHI	
ABORST2	RISKCONT	AARON BORST	ABNCHI	
ABOYD1	FXTRADER	ALISTAIR BOYD	INST	
ABOYD2	FXTRADER	ALISTAIR BOYD	INST	Change to Inquiry Only
ABUDHWA1	ERGENCY	AMIN BUDHWANI	ABNCHI	
ABUDHWA2	ERGENCY	AMIN BUDHWANI	ABNCHI	
ACOOPEP	WBFXTRDR	AMY COOPER	ABNCHI	
ADIDIE1	FXTRADER	ANNA DIDIER	MJRS	
ADIDIE2	FXTRADER	ANNA DIDIER	FXTOT	Change to Inquiry Only
ADIDIE3	FXTRADER	ANNA DIDIER	FXTOT	Delete
ADIDYCH1	RISKCONT	ALEX DIDYCH	ABNCHI	
ADIDYCH2	RISKCONT	ALEX DIDYCH	ABNCHI	
AJAYAVE1	INQ	ANURADHA JAYAVEL	MM	
AJAYAVE2	INQ	ANURADHA JAYAVEL	ABNCHI	
AKADAM1	ERGENCY	AJAY KADAM	ABNCHI	
AKADAM2	ERGENCY	AJAY KADAM	ABNCHI	
AKAMATH1	INQ	AJAY KAMATH	ABNCHI	
AKAMATH2	INQ	AJAY KAMATH	ABNCHI	
AKHAN1	FXTRADER	ABDULLAH KHAN	EXOT	
AKHAN2	FXTRADER	ABDULLAH KHAN	EXOT	Change to Inquiry Only
ALAMET1	BOMNGR	AVRUM LAMET	FXTOT	
ALAMET2	INQ	AVRUM LAMET	FXTOT	
ALAMET3	INQ	AVRUM LAMET	FXTOT	
ALOBOMO1	FXTRADER	ARMANDO LOBO MORALES	CORP	
ALOBOMO2	FXTRADER	ARMANDO LOBO MORALES	CORP	Change to Inquiry Only
AMALANI1	INQ	AMITH MALANI	ABNCHI	
AMALANI2	INQ	AMITH MALANI	ABNCHI	

1. The FXTRADER and WBFXTRDR functional template were asked to be modified.
2. We also found one interesting issue – Stefan Frieberg (SFRIEB) and Daniel Gonzalez (DGONZAL) have the same template (SECADMIN) but have different conflicts.

3. As for the INQ template - we will need to see whether "SWIFT MESSAGE HANDLER" can be removed or not (See **Table 3**)

TABLE 3
ID STRUCTURE AFTER PROJECT



USER_ID	FUNC_TMPLATE	USER_NAME	ORG_TEMPLATE
AARON02	FXTRADER	ABEL ARONOVITZ	INST
AAUSTR1	BOMNGR	AUDREY AUSTREVICH	FXTOT
AAUSTR2	INQ	AUDREY AUSTREVICH	FXTOT
AAUSTR3	INQ	AUDREY AUSTREVICH	MM
ABORST1	RISKCONT	AARON BORST	ABNCHI
ABORST2	INQ	AARON BORST	ABNCHI
ABOYD1	FXTRADER	ALISTAIR BOYD	INST
ABOYD2	INQ	ALISTAIR BOYD	INST
ABUDHWA1	ERGENCY	AMIN BUDHWANI	ABNCHI
ABUDHWA2	INQ	AMIN BUDHWANI	ABNCHI
ACOOPE	WBFXTRDR	AMY COOPER	ABNCHI
ADIDIE1	FXTRADER	ANNA DIDIER	MJRS
ADIDIE2	FXTRADER	ANNA DIDIER	FXTOT
ADIDIE3	INQ	ANNA DIDIER	FXTOT
ADIDYCH1	RISKCONT	ALEX DIDYCH	ABNCHI
ADIDYCH2	INQ	ALEX DIDYCH	ABNCHI
AJAYAVE1	INQ	ANURADHA JAYAVEL	MM
AJAYAVE2	INQ	ANURADHA JAYAVEL	ABNCHI
AKADAM1	ERGENCY	AJAY KADAM	ABNCHI
AKADAM2	INQ	AJAY KADAM	ABNCHI
AKAMATH1	INQ	AJAY KAMATH	ABNCHI
AKAMATH2	INQ	AJAY KAMATH	ABNCHI
ALAMET1	BOMNGR	AVRUM LAMET	FXTOT
ALAMET2	INQ	AVRUM LAMET	FXTOT
ALAMET3	INQ	AVRUM LAMET	FXTOT
ALOBOMO1	FXTRADER	ARMANDO LOBO MORALES	CORP

4. As far as the OMRSSC template is concern – it was discussed, whether we should consider removing the "OPTIONS/FUTURES CALENDAR....." function.

After all the changes and modifications, the end result according to the Sarbanes Oxley Act of 2002 should be so that the application controls are embedded within software programs to prevent or detect unauthorized transactions. When combined with other

controls, as necessary, this and all application controls ensure the completeness, accuracy, authorization and validity of processing transactions.

Logical Security Control

OMR does not display a message to users upon login that "access is only allowed for authorized users."

Mitigating Control -- the VMS Operating System logon displays a message

OMR does not display to users upon login the date and time they last logged in.

Mitigating Control -- OMR can generate a "Last Login" report

1. Periodic Access Reviews

Listings of OMR users sent to their respective managers on a quarterly basis are not system-generated from the application. Individual Excel spreadsheets are maintained throughout the quarter based on users added, modified, and removed from OMR.

Mitigating Control – There should be reconciliation to the prior quarter's spreadsheets and management responses is performed.

2. User account removal

Access is not terminated immediately when users left the bank. Even business users' request account to be removed, but the request is not always being executed.

Mitigating Control -- Please submit the user request form to remove access immediately when Front Office users leave the bank or change groups.

Note: OMR ID needs to remove immediately, while the associated profit center can remain open. Desk Managers will review the user access list quarterly to validate the action is being taken correctly. (Appendix D)

CONCLUSION

After going through the various “Conflict Reports” with senior management and the department heads, the following conclusions were reached:

On the Business side:

- a. All users must be transitioned to the Separation of Duties business model as outlined by Sarbanes Oxley Act (SOXa). This process will be ongoing through March 2009, starting with the Opti Management Resources (OMR) application and in phases to all other applications. Modify user lifecycle management process to include Separation of Duties components and a somewhat seamless transition of users to the Separation of Duties model.
- a. Define and assign enterprise roles describing the responsibilities and access required in order to support a long term access control approach.
- b. Execute the Separation of Duties processes.

On the Information technology:

- a. Design, develop and configure technology to support access reporting to meet Separation of Duties requirements.
- b. To enhance application reporting. Deploy reporting technology to application and business areas based on business risk.
- c. Integrate the conflict management tool into company business model. Deploy Separation of Duties technology to applications and business areas based on business risk.

- d. Roll out Separation of Duties approach to remaining SOX and non-SOX applications based on business risk.
- e. Application controls are embedded within software programs to prevent or detect unauthorized transactions. When combined with other controls, application controls ensure the completeness, accuracy, authorization and validity of transaction processing. [\[5\]](#)
 - Account balancing activities
 - Check digits
 - Predefined data listings
 - Data reasonableness tests
 - Logic tests

Several steps were also undertaken, or at least presented, in order to maximize security and data integrity for the long-term across all platforms:

1. Assume that someone out there will intentionally try to break your application and may have access to greater resources than you expended in developing it.
2. Assume that you will receive erroneous data from authorized, authenticated users, and develop a way to deal with it.
3. If you choose to use client-side input validation, ensure that the input is also validated at the server end.
4. Be careful with application component privileges. Always apply the minimum possible permissions needed to carry out any particular task.

5. Never allow passwords or user specific details to be passed in plain-text to the client browser or between application components.
6. Ensure that confidential system information is not encoded into documents that could potentially be accessed by a remote client, either directly or through escalated application component permissions and calls.
7. Take extreme care with file permissions and access rights.
8. Remove all unnecessary material from the hosting servers and only install services that are required for the application/system to function.
9. Remove all comments and unnecessary information from client-side code.
10. Distribute application functions between servers when possible to limit data access from a compromised host.
11. Where possible, only use shared resources you have direct control over. If this is not possible, ensure appropriate checks for data integrity are made.
12. Test the application thoroughly.
13. Get a third party to perform an independent assessment both of the application's security and the system's host servers before going live.

The security threats and responses to ABN AMRO's infrastructure and banking software components are commonly understood, and classical security assessment or "ethical hacking" methodologies are adept at increasing the security level of its key infrastructure components. [\[15\]](#) However, custom application code is often untested, and attackers are now focusing upon these security flaws to compromise system components or otherwise gain access to confidential data. For these reasons, organizations like ABN

AMRO are trying to ensure that appropriate security assessments are carried out on all custom, in-house developed, applications. Getting financial institutions like ABN AMRO to finance security projects like this takes some persuasion.

Financing Security in the Bank

Finding a way to implement these new security processes financially was almost a show stopper, under regulatory and threat pressures, financial institutions like ABN AMRO Bank look for ways to fund, and market, security:

SEPTEMBER 13, 2006 | NEW YORK [\[16\]](#)-- Financial services companies are not only finding innovative ways to implement new security initiatives, they're also finding innovative ways to fund them.

ABN AMRO Bank N.A. now requires all the bank's application projects to allocate one percent of their funding to their security. It's all part of a movement among financial institutions to build security into services from the ground up.

Joe Bernik, CISO for La Salle Bank and head of information security for ABN AMRO Bank, N.A., says this ensures that a new application goes hand in hand with the organization's security, and the security aspect gets funded.

"If you have to mitigate security risk after the fact, it's a costly exercise," Bernik told attendees of the Cyber Security Executive Summit here today.

CISOs and risk management officials at major financial institutions speaking here say they are struggling to keep up with emerging threats and the ever-changing regulatory landscape. They face not only phishing exploits, but emerging application-level security

issues, client laptop security, and compliance with regulations like strong authentication for online banking, which banks must deploy by the end of the year, according to FFIEC regulations.

But even with the progress firms like ABN AMRO have made in folding security into the application and service development process, there's still a long way to go. Bernik says his company is "trying" to routinely perform risk assessments on projects before they go live. "With risk assessment, when you do the assessment, you have to be in pre-production or something that's ready to be embedded in the app."

Regs like SOX have made it easier to get funding for security, CISOs say. "The regulators are doing the job for me" of getting the business side to take security more seriously, Bernik said. "I've had challenges in my business getting business owners to listen and take heart" in implementing security controls. The FFIEC's authentication reg is one such example, he said. But as the regulatory buying craze slows down, financial organizations no longer have that ammunition, according to C. Warren Axelrod, senior vice president and business information security officer for the United States Trust Company. "You could say 'do it or the regulators will come in,'" he said. "But that's not so true now."

Banks are weighing the cost of strong authentication: Token-based authentication may make sense internally, but not for consumers, they say. "You're not going to pay \$30 to \$40 for each of your millions of customers," Axelrod said. Banks are looking for easy-to-use, simpler options for authentication, he said.

Getting funding for security is not just a matter of folding it into projects from the get-go, but also making it a selling point for your customers, financial execs say. Some large banks such as Bank of America, with its Passmark security, have already begun using security as a marketing tool.

"It's not about looking at point solutions," said Don Rhodes, policy manager for payments and technology at the American Bankers Association. "Think federated identities -- so that it's a revenue-steering solution and not a cost" issue, he said.

The bottom line is, for banks and financial services it's more about customer confidence in security. And marketing edge aside, it's a financial community issue. If one bank loses customer confidence, it hurts the entire banking system, says Dan Shutzer, executive director of the Financial Services Technology Consortium.

APPENDICES

Appendix A: RESULTS FROM CONFLICT REPORTS

A. General File Count

Description	Observations
NUMBER OF RECORDS IN RAW USER FILE*	591
NUMBER OF RECORDS IN RAW SECURITY FILE	3370
NUMBER OF RECORDS IN MAPPING FILE	974

***NOTE1:** OMR users have multiple user IDs to allow for processing multiple transactions concurrently (e.g., Bsmith1, Bsmith2). For the purposes of this analysis a Main User ID was created to hold the root user ID minus the numeric.

B. User Specific Counts

Description	Observations
NUMBER OF UNIQUE USER NAMES IN USER FILE	292
NUMBER OF UNIQUE USER IDS IN USER FILE	292
NUMBER OF USER NAMES WITH "EODPROCP" IDS WITH NO REGULAR ID MATCH	0
NUMBER OF UNIQUE USER IDS WITH TRANSACTIONS	292
NUMBER OF UNIQUE USER IDS WITH MAPPED FUNCTIONS/TRANSACTIONS	237
NUMBER OF UNIQUE USER IDS WITH REMOVAL FUNCTIONS / VIEW ONLY TRANSACTIONS	55

C. Conflict Counts

Description	Observations
PROGRAM HAS LOOPED THROUGH ALL CONFLICTS FOR EACH USER	1
TOTAL NUMBER OF CONFLICTS IN CONFLICTS MATRIX	150
NUMBER OF UNIQUE CONFLICTS IDENTIFIED	57
NUMBER OF UNIQUE CONFLICTS IDENTIFIED FOR ALL USERS	2,031
NUMBER OF USERS WITH IDENTIFIED CONFLICTS	156

This information was taken to the meeting with senior management and department heads to go over the results of the reports.

Appendix B:
SAMPLE OMR CONFLICT MATRIX

Activity Number	Activity	Price Trades/Analytics (FO)	Manage Positions/Funding Requirements (FO)	Input trades (FO))	Enrich trades information for settlement (BO)
1	Price Trades/Analytics (FO)				
2	Manage Positions/Funding Requirements (FO)				
3	Input trades (FO))				
4	Enrich trades information for settlement (BO)	X	X	X	
5	Release Trades (BO)	X	X	X	X
6	Confirm Trades (BO)	X	X	X	
7	Amend Trades		X	X	X
8	Settle Trades (BO)	X	X	X	X
9	Update/Amend EOD Market Prices	X	X	X	X
10	Add/Amend Static Data (RDM)	X	X	X	X

SAMPLE NON-CONFLICTING TRANSACTIONS (GENERALLY VIEW ONLY)

ALL PRODUCTS POSITIONS ZOOM SCREEN....
CASH FLOW ONLINE SCREEN WITH GRAPH....
CASH POSITIONS GAP/LIQUIDITY SCREEN...
CND CASH FLOW / SUMMARY SCREEN.....
COLLATERAL PORTFOLIO SCREEN.....
CONSOLIDATED CASH POSITIONS SCREEN....
CUMULATIVE REVERSE GAP SCREEN W/LIMITS
FIXED INCOME AND STOCK PORTFOLIO SCR.N.
FORWARDS BY CURRENCY PAIR BY GAP SCR.N.
FRA/FUTURES PRICING SCREEN.....
FX DAILY POSITIONS.....
FX FORWARD POSITIONS.....
FX LIQUIDITY BY GAP SCHEDULE SCREEN...
GAP INTEREST RATE RISK ONLINE SCREEN..
IMPLIED SPOT BY GAP SCHEDULE SCREEN...
INTEREST RATE FUTURES AND OPTIONS.....
INTEREST RATE POSNS BY GAP SCHEDULE...
OCP BREAK EVEN RATES SCREEN.....
OCP SELECTED CURRENCY DETAIL.....
OCP SELECTED CURRENCY SCREEN.....
ONLINE SCREEN.....
OPTIONS POSITION MANAGEMENT SCREEN....
PORTFOLIO POSITION BOND EQUIVALENCE...
PORTFOLIO POSITION ECONOMIC ANALYSIS..
PORTFOLIO POSITION ONLINE SCREEN.....
PROJECTED CASH POSITIONS SCREEN.....
SECURITIES CASH SETTLEMENT DETAIL.....

Appendix D:

SAMPLE TRANSACTION SYSTEM OWNERS FLAGGED FOR DELETION (BY USER)

MAIN USER ID	USER NAME	OMR USER ID	TEMPLATE	LEVEL1	TRANSACTION
CASKIN	CAMILLE ASKINS	CASKIN1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
CMACK	CHERYL MACK	CMACK1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
HJAIN	HEMANT JAIN	HJAIN1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
JFREUND	JESSE FREUND	JFREUND1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
KCARTE	KARON CARTER KESAVAN	KCARTE1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
KRAGHUN	RAGHUNATHAN	KRAGHUN1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
MARARUL	MARY ARUL P.	MARARUL1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
PHARIHA	HARIHARANANDANAN PREMKUMAR	PHARIHA1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
PVASURA	VASURAO	PVASURA1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
RPOOKAT	RAKESH POOKAT SANDIP	RPOOKAT1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
SBHATTA	BHATTACHARYA	SBHATTA1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK CATEGORIES.....
CASKIN	CAMILLE ASKINS	CASKIN1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....
CMACK	CHERYL MACK	CMACK1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....
HJAIN	HEMANT JAIN	HJAIN1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....
JFREUND	JESSE FREUND	JFREUND1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....
KCARTE	KARON CARTER KESAVAN	KCARTE1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....
KRAGHUN	RAGHUNATHAN	KRAGHUN1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....
MARARUL	MARY ARUL P.	MARARUL1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....
PHARIHA	HARIHARANANDANAN PREMKUMAR	PHARIHA1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....
PVASURA	VASURAO	PVASURA1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....
RPOOKAT	RAKESH POOKAT SANDIP	RPOOKAT1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....
SBHATTA	BHATTACHARYA	SBHATTA1	STATIC	MULTI CURRENCY TRADE PROCESSING	RISK GROUPS.....

APPENDIX E:

SUMMARY OF CONFLICTS AND NUMBER OF USERS ASSOCIATED WITH CONFLICTS

ACTIVITY 1 DESCRIPTION	ACTIVITY 2 DESCRIPTION	NUMBER OF USERS WITH CONFLICT
AMEND TRADES	INPUT TRADES (FO))	156
AMEND TRADES	MANAGE POSITIONS/FUNDING REQUIREMENTS (FO)	104
ADD/AMEND STATIC DATA (RDM)	INPUT TRADES (FO))	65
ADD/AMEND STATIC DATA (RDM)	CONFIRM TRADES (BO)	65
ADD/AMEND STATIC DATA (RDM)	AMEND TRADES	65
CONFIRM TRADES (BO)	INPUT TRADES (FO))	65
AMEND TRADES	CONFIRM TRADES (BO)	65
ADD/AMEND STATIC DATA (RDM)	RELEASE TRADES (BO)	64
RELEASE TRADES (BO)	INPUT TRADES (FO))	64
AMEND TRADES	RELEASE TRADES (BO)	64
ENRICH TRADES INFO FOR SETTLEMENT (BO)	INPUT TRADES (FO))	63
AMEND TRADES	ENRICH TRADES INFO FOR SETTLEMENT (BO)	63
ADD/AMEND STATIC DATA (RDM)	UPDATE/AMEND EOD MARKET PRICES	51
UPDATE/AMEND EOD MARKET PRICES	INPUT TRADES (FO))	51
UPDATE/AMEND EOD MARKET PRICES	AMEND TRADES	51
ADD/AMEND STATIC DATA (RDM)	ENRICH TRADES INFO FOR SETTLEMENT (BO)	50
RECONCILE NOSTROS/CASH (BO)	ADD/AMEND STATIC DATA (RDM)	50
RECONCILE NOSTROS/CASH (BO)	INPUT TRADES (FO))	50
RECONCILE NOSTROS/CASH (BO)	ENRICH TRADES INFO FOR SETTLEMENT (BO)	50
RECONCILE NOSTROS/CASH (BO)	RELEASE TRADES (BO)	50
RECONCILE NOSTROS/CASH (BO)	CONFIRM TRADES (BO)	50
RECONCILE NOSTROS/CASH (BO)	AMEND TRADES	50
RECONCILE NOSTROS/CASH (BO)	UPDATE/AMEND EOD MARKET PRICES	50
RECONCILE AND REPORT P/L (FINANCE)	ADD/AMEND STATIC DATA (RDM)	50
RECONCILE AND REPORT P/L (FINANCE)	RECONCILE NOSTROS/CASH (BO)	50
RECONCILE AND REPORT P/L (FINANCE)	INPUT TRADES (FO))	50
RECONCILE AND REPORT P/L (FINANCE)	ENRICH TRADES INFO FOR SETTLEMENT (BO)	50
RECONCILE AND REPORT P/L (FINANCE)	RELEASE TRADES (BO)	50
RECONCILE AND REPORT P/L (FINANCE)	CONFIRM TRADES (BO)	50
RECONCILE AND REPORT P/L (FINANCE)	AMEND TRADES	50
RECONCILE AND REPORT P/L (FINANCE)	UPDATE/AMEND EOD MARKET PRICES	50
RELEASE TRADES (BO)	ENRICH TRADES INFO FOR SETTLEMENT (BO)	50

References

Picture on the front cover was taken from Nawara Group website:

<http://www.nawaragroup.com/images/> April 4, 2008

[1] Quoted from the Legal Issues Course, Lewis University. Instructor Gary Bannister, 11th September 2007.

[2] Quoted from the Legal Issues Course, Lewis University. Instructor Gary Bannister, 29th August 2007.

[3] Quoted from the website: www.sarbanes-oxley-101.com/sarbanes-oxley-compliance.htm, March 3rd, 2008

[4] Quoted from the website: www.sarbanes-oxley-101.com/sarbanes-oxley-compliance.htm, March 3rd, 2008

[5] Quoted from the Legal Issues Course, Lewis University. Instructor Gary Bannister, 11th August 2007

[6] Quoted from the website: www.abnamro.com/about_our_bank/then_and_now.htm, March 14, 2008

[7] Quoted from the website: www.btquarterly.com/?mc=segregations-duties. March 17, 2008

[8] Quoted from the website: www.searchsecurity.techtarget.com/ written by Shon Harris March 26, 2008

[9] Quoted from the website: www.searchsecurity.techtarget.com/ written by Shon Harris March 26, 2008

[10] Quoted from the website: www.btquarterly.com/?mc=segregations-duties.

March 26, 2008

[11] Quoted from the website: www.btquarterly.com/?mc=segregations-duties.

March 26, 2008

[12] Quoted from the website: www.cioupdate.com/trends/article.php/ March 26, 2008

[13] Quoted from the website: www.cioupdate.com/trends/article.php/ March 26, 2008

[14] Quoted from the website: www.boran.com/security/ April 2, 2008

[15] Quoted from the website: www.technicalinfo.net/papers/ on April 3rd, 2008.

Written by Gunter Ollmann

[16] Quoted from the website: www.darkreading.com/document.asp?doc_id=103706
on April 3rd, 2008. Written by Kelly Jackson Higgins, Senior Editor, Dark Reading

[17] Quoted from the website: www.sarbanes-oxley.be/sarbanes-oxley_process.html
on April 4th, 2008.