Raz-Lee Security
White Paper

Basel II and iSeries
Security, Audit and Compliance

June 2008

iSecurity
Distributed by **AH Technology Pty Ltd**
In Australia, New Zealand and South East Asia

www.ahtechnology.com.au Email: **info@ahtech.com.au** Phone: **+61 3 9885 4877**

Raz-Lee Security is the developer of *iSecurity*
A suite of iSeries security products

Legal notice: This document reflects the understanding of Raz-Lee Security of iSeries SECURITY and AUDIT compliance with the Basel II operational risk requirements. While Raz-Lee believes that adopting the measures recommended in this white paper will considerably increase iSeries compliance with Basel II, we are not in a position to guarantee that the implementation of the above recommendations ensures a complete and full compliance with ALL aspects of Basel II. The information provided is of general nature and users must undertake their own research and advice to satisfy their required level of compliance with Basel II.

Basel II- An Introduction

Background:

Bloor Research, in a paper written by Fran Howarth and released on August 16, 2005, stated the following:

"The Basel II capital adequacy framework is a regulatory tool that is designed to help mitigate the risk that haunts financial institutions. Its designers had a clear purpose in mind: to create safer and sounder financial institutions by mandating that the amount of capital that they hold offsets the risks inherent in the banking system.

Risks to financial institutions are traditionally classified as three-fold: credit risk, market risk, and operational risk. In development since 1999 and building on the Basel I directive on capital adequacy as well as bank supervision legislation, the rules for the Basel II directive were finally agreed in July 2004. Back in 1998, when Basel I was ratified, banks were wrestling with bloated loan portfolios and credit risk loomed as banking's big bugbear. But the world of finance has become increasingly complex, exposing banks to greater risks than ever before. To overcome this, the Basel II framework aims to enhance the transparency of financial institutions' operations and to support a level playing field in an increasingly integrated global financial system."

Basel II and IT:

Of the three risk areas outlined above, credit risk, market risk and operational risk, we will concentrate on the latter as it is the most directly related to our topic.

As operation risk by nature is intimately tied in with IT procedures and policies, we will quote still another sentence or two from the Bloor Research paper as follows::

"From an IT perspective, financial institutions must take a more advanced risk management stance that focuses on business data and works to increase the quality, consistency, auditability, and transparency of data. In particular, the Basel II framework aims at grounding risk measurement and management into actual data and formal quantitative techniques…"

Indeed, in this paper we will focus on Raz-Lee Security's iSecurity product for protecting IBM midrange Server i5 systems against intrusions, misuse and other assorted security-related issues which can easily undermine the integrity of a financial institutions critical business data and, as such, undermine the institutions compliance with the all-important Basel II regulations.

We will relate to the modules making up iSecurity using the framework suggested by Bloor Research.

COBIT, Base II & iSeries Security Policies

While Basel II is aimed at ensuring a low level of operational risk to financial institutions, it down not spell out in clear terms the guidelines by which such a financial institution should actually implement such operational risk controls and restraints.

As such, many in the security and audit field turn to the guidelines development under the name of Control Objectives for Information and related Technology (COBIT®) developed by the USA based IT Governance Institute (ITGI) (www.itgi.org).

The ITGI website states: "COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations."

This document describes the Basel II objectives considered by us as the most relevant to iSeries Security, Audit and Compliance. Where applicable, the document provides references to iSecurity functions that can be useful in achieving the required level of compliance to Basel II requirements. It is recommended that iSeries users gain access to Basel II documentation to appraise the complete list of requirements.

iSeries Sites

The iSeries comes equipped with a significant number of security tools built-in to its Operating System. Such tools cover areas like object level security, built in logging (Journals including the Security Audit Journal, message queues, history log etc), and built in monitoring (message queues etc.).

This document only refers to the 'technical' aspects of implementing the guidelines. Many other documents are available containing suggestions and recommendations regarding available methodologies for a corporation to implement in order to achieve the required level of compliance.

Many sites are using the iSecurity software to complement native iSeries tools. The relevant Basel II requirements where users can draw benefits from the use of iSecurity are listed below.

Basel II Requirements Summary

IMPORTANT

1. **High Exposure**
   In a case where
   a. An iSeries system has an ERP application that enables its users to view, copy, change, and delete its objects (many green screen applications do this) and…
   b. It also possible to access the iSeries using TCP/IP access protocols such as FTP, SQL, ODBC, DDM and others using tools such as MS Access, MS Excel, IBM iSeries Access etc. (most sites allow such access)

   Application data can be viewed, copied, changed or deleted with the operating system offering no mechanism to protect, log or report such transactions.

2. **Non Compliance with Basel II**
   When a financial application has the above exposures, the iSeries system is **NOT COMPLIANT** with Basel II requirements.

   Basel II clearly requires that a system MUST be able to identify any attempt to modify a financial record.

Table 1: Basel II Objectives Description and iSecurity Relevant Functions

COBIT/Basel II Objective	iSecurity Functions that can increase compliance
Manage Security Measures	Firewall, Password, Audit, Action, User Management, Visualizer
Identification, Authentication, Access	Firewall, Password, Audit, Action, User Management, Visualizer
Security of Online Access to Data including quality, consistency, auditability and transparency of business data	View, Capture and Journal for data access. Also Firewall, Audit, Action for improved escalation and response. (*) Please review this section for object authority discussion and IMMEDIATE NON COMPLIANCE.
Management Review of User Accounts	Audit, Action, Assessment
Security Surveillance	Firewall, Audit, Action, Capture
Violation and Security Activity Reports	Firewall, Audit, Action
Protection of Security Functions	Firewall, Audit, Action, Anti Virus
Malicious Software Prevention	Firewall, Audit, Action, Anti Virus

Discussion by Basel II Objectives

As stated above, COBIT "enables clear policy development and good practice for IT control throughout organizations". In particular, COBIT® 4.0 emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment, simplifies implementation of the COBIT framework and, in doing so, facilitates Basel II compliance.

Quotes which appear below are taken from the appropriate COBIT directives.

1. Manage Security Measures

This objective addresses the need for establishing an IT security implementation which ensures that security policies and their implementations satisfactorily meet business objectives and risk exposures.

This objective requires not only implementation of the security policies but also regular checks to ensure the on going compliance of the system setup with the policies.

iSecurity Firewall, Audit & Action, Assessment

1. **Firewall** can be used to manage, control and protect access to company data from all TCP/IP access points into the system (ODBC, FTP, SQL, iSeries Access, MS Access, MS Excel etc.). **Firewall** can log all approved and rejected activities, produce reports as required, and, using the interface with **Audit** and **Action**, deliver immediate escalation via email, SMS etc. as well as real time response to threats.
2. The **iSecurity Assessment** module should be involved on a regular basis to ensure system setup has not changed.

2. Identification, Authentication, and Access

"The logical access to and use of IT computing resources should be restricted by the implementation of adequate identification, authentication, and authorization mechanisms, linking users and resources with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections, and other system (network) entry ports from accessing computer resources."

Firewall (including Password Manager), Audit and Action

1. Use **Password** manager and OS system values to ensure inactive users are disabled; passwords are changed regularly and trivial password construction is not possible.
2. Use **Firewall** to address all issues of network TCP/IP access (see item 1 above) to deliver an Intrusion Protection Solution (IPS) with **Audit** and **Action** delivering an Intrusion Detection Solution (IDS) - immediate escalation and real-time response to threats. **Firewall's** flexibility allows setting up specific rules to ensure sensitive data is accessed only by the authorized person (linking a task to a specific IP address, disallowing access to data from outside the office, etc.).

3. Security of Online Access to Data

"IT management should implement procedures in line with a security policy that provides access and security controls based on the individual's demonstrated need to view, add, change, and delete data."

Firewall (see also responses to items 1 and 2 above)

1. This objective requires that, in a networked environment, security should be implemented so that access to data via authorized personnel is such that where ever possible the highest level of granularity should be adopted to ensure the user can perform no more than is required. Example: Only read data, but not update or delete.

2. Use **Firewall** to address all issues of network TCP/IP access (see item 1 above) to deliver an Intrusion Protection Solution (IPS). The iSeries OS enables further granularity by allowing the software to separately control different actions (verbs) like: READ, WRITE, DELETE, RENAME. CREATE OBJECT, CREATE LIBRARY.

   DANGER: Without TCP/IP protection (via software such as Firewall), your AS/400, iSeries system is **NON COMPLIANT WITH Basel II** if the following conditions exist:

   a. Each and every legitimate user of an application has object authority to read (view), change, copy or delete data records.
   b. The application is a **financial** application.

   Without TCP/IP exit point protection, users with the above authority can gain TCP/IP access to alter existing financial records. Basel II requires the ability to identify any attempt to change financial records.

   Native i5/OS DOES NOT provide a mechanism to manage, control and protect data against TCP/IP transactions (FTP, ODBC, SQL, DDM using tools such as MS Access, MS Excel, IBM iSeries Access, FTP from DOS prompt etc.).

   DANGER: If your financial application is a **green screen application,** there is a **GRAVE CHANCE** your system is **NON COMPLIANT** with Basel II!

3. Use **View** to selectively hide either entire records, or data in selected fields within records, from selected users, without having to make changes to applications. Online GUI interface is used to define criteria for hiding records/fields.

4. **Capture** can be used to record green-screen images of user activity. Such captured sessions can be initiated as a routine deterrence, or can be initiated dynamically by the **Action** module, upon detection of a possible security threat, such as access to a protected file or working after-hours. Captured session logs can be archived for legal purposes, and searched at a later date for application-specific information determined to be suspect.

5. **Journal** provides the capability to generate a history "time-line" activity report of a particular entity in an application (customer number, patient number, mortgage number, etc.), collated from all iSeries data files making up the application. Journal provides a before and after image of records, lending to accountability and traceability of application events and changes.

4. Management Review of User Accounts

"Management should have a control process in place to review and confirm access rights periodically. A comparison of resources with recorded accountability should be made to help reduce risk of errors, fraud, misuse, or unauthorized alteration".

iSecurity Assessment Module, Audit and Action

1. There are a number of **iSecurity** features which address this requirement. Start with the **iSecurity Assessment** module to record your current settings. Review and change as required, meeting your business objectives and security policies. Run the **iSecurity Assessment** again and keep as your baseline reference. From then on, execute the **iSecurity Assessment** module on a regular basis and compare its reports to your baseline reference.

2. As a complementary measure, use **Audit** and **Action** to monitor all settings they can detect (System values). Set the software to escalate alerts when a setting is changed.

5. Security Surveillance

"IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner".

Firewall, Audit and Action

1. **Firewall** ensures every TCP/IP activity is logged and reported. With **Audit** and **Action**, you can ensure that an attempt to violate security is escalated immediately with the corrective or preventive action taken in real-time.

2. **Audit** and **Action** deliver the same result when monitoring the Security Audit Journal as well as system events and messages.

3. **Capture** (see 3.4 above).

6. Violation and Security Activity Reports

"IT security administration should ensure that violation and security activity is logged, reported, reviewed, and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need-to-know."

Firewall, Audit and Action

1. Please refer to information in objective item 6 above. **Firewall**, **Audit** and **Action** can all provide regular reports (in any time interval required) in addition to continuous monitoring, immediate detection, escalation and response.

7. Protection of Security Functions

"All security related hardware and software should at all times be protected against tampering to maintain their integrity and against disclosure of secret keys. In addition, organizations should keep a low profile about their security design, but should not base their security on the design being secret."

Firewall, Audit, Action and AntiVirus

1. **Firewall** can be used to ensure no unauthorized access via the network can update / delete / insert data into files. The **Anti**-**Virus** module can perform on going detection protection and immediate removal of viruses.

8. Malicious Software Prevention

Detection and Correction

"Regarding malicious software, such as computer viruses or Trojan horses, management should establish a framework of adequate preventative, detective, and corrective control measures, and occurrence response and reporting. Business and IT management should ensure that procedures are established across the organization to protect information systems and technology from computer viruses. Procedures should incorporate virus protection, detection, occurrence response, and reporting."

iSecurity Anti Virus, Firewall, Audit & Action

1. Use the **Anti Virus** module to ensure viruses and malicious code are detected and removed as soon as it is possible.
2. **Firewall** will secure files from unauthorized attempts via the network to change or delete data.