



ISSUE 1

VOL 6

JAN 2008

Solutions *are our business*

11301 NORTH US HIGHWAY 301, SUITE 106
THONOTOSASSA, FL 33592
(813) 246-4757 • (813) 246-4576 (FAX)
WWW.AASYSGROUP.COM

AaSys Undergoes FFIEC Review

AaSys is in the final phase of an IT and Security Audit being conducted by an independent third party CPA firm. This FFIEC Review and Assessment includes the review of security controls, policies, and procedures pertaining to AaSys' IT Services. This audit is designed to provide reasonable assurance of detecting material errors or irregularities in the areas of:

- **Quality Review** - Review policies, standards, and procedures to determine if the data processing systems are efficiently controlled and if regulatory requirements are satisfactorily addressed.
- **Compliance Review** - Review adherence to established policies, standards and procedures.
- **Integrity Review** - Review fraud detection/deterrence practices, application program and operating system integrity,

application system implementation, and monitoring employee activities to determine if the potential for unauthorized activities has been reduced to acceptable levels.

The audit has been performed in compliance with the Federal Financial Institution Examination Council (FFIEC) procedures. In performing the audits, applicable policies, procedures, and security controls have been tested in the areas of:

- Management
- Computer Operations (*Includes Help Desk/User Support Operations*)
- Business Continuity Planning
- Information Security

A final report is scheduled to be released this month.



Check this out....!

Need some extra power for your laptop or to charge your phone on the road? The **I-Tec 200 Watt Power Inverter with USB Port** has two outlets, another cigarette adapter and even a USB port outlet! Plus it fits right in a cup holder! This nifty device converts your vehicle's 12 volt power to household 110 volt power; powers up to 1.8 amps. Never have a dead cell phone or laptop again!



GLBA Risk Assessment

AaSys will evaluate every aspect of business operations and IT procedures, to the following Evaluation Criteria:

STRATEGY –

- Is the program comprehensive and does it “fit” the organization?
- Does the program have clear objectives and directions?
- Does the program have enterprise-wide coverage?
- Is the program adequate?
- Is the program coordinated across functional areas?

MANAGEMENT –

- Is an appropriate individual designated with responsibility for the program?
- Are there clear reporting lines for staff functions?
- Does executive management demonstrate support for the program?
- Are there processes in place that demonstrate management oversight?

IMPLEMENTATION –

- Is the program adequately documented (policies, manuals, guidelines, etc)
- Are processes consistently implemented across the organization?
- Is there evidence of employee awareness?
- Are there processes in place to review and monitor the program?
- Is the program supported with adequate training and instruction?

TECHNOLOGY/OPERATIONS –

Do tracking and reporting systems provide sufficient detail and coverage? Are systems and processes independently reviewed/evaluated?

Are technical controls and safeguards in place and upgraded as needed?

Are supporting applications and tools tested/updated for reliability, accuracy and efficiency?

Finally, identified threats are classified according to the likelihood of occurrence as well as the potential impact to the bank.

Most importantly, Security Controls to address vulnerabilities within the organization will be provided. Security Controls provide procedures to mitigate or eliminate vulnerabilities.

After gathering data and detailing our findings, AaSys will submit a draft report to our designated contact. Feedback will then be incorporated into our results, and final reports will be provided to management. Collaterals consist of two reports, a broad Executive Report and a detailed Technical Report.

DELIVERABLES -

The finalized reports provide a broad overview of the goal of the engagement, how the study was conducted, and our results. Documentation will identify vulnerabilities and the associated risk. The appropriate Security Controls for each vulnerability will be identified. Finally, a numeric score (percentage) will be assigned for each Evaluation Criteria in each of the eleven categories (domains).

Part 2 – Ongoing Risk Assessments Performed by the Organization

The regulatory organizations are becoming more insistent that risk assessments should be considered an ongoing process and not a onetime event. Moreover, the banks themselves are being charged with the responsibility to perform these assessments, assess weaknesses and take steps to mitigate risks.

What complicates this requirement for many organizations is the absence of a framework on which to base the risk process. Commercial packages available often come with pricey hardware requirements and the technical knowledge need to deploy and support such solutions is often prohibitive.

AaSys has contracted with SourceSentry in utilizing their OneComply web based solution for conducting all ISO17799 Risk Assessments. The application and the results will be hosted on a secure server hosted at AaSys and the bank will receive a one year license for use of OneComply. A portal requiring a user name and password will be established and an SSL connection will further secure access to the application.

OneComply is a tool that allows financial institutions to assess compliance, track activities and measure internal controls. Using the framework provided by OneComply, an organization’s focus moves away from when and how to complete an assessment and instead focuses on the remediation of identified risks. OneComply provides for consistent standards to be applied throughout all phases of the organization’s processes.

Pricing and additional information can be obtained by contacting your Account Manager.

Part 1 – Independent Third Party Review Conducted by AaSys

The goal of this engagement is to assess the Operational Risk posture of the organization. Operational Risk is defined by the Basel Committee as “the risk of loss resulting from inadequate or failed internal processes, people and systems from external events”.

This Risk Analysis will identify potential threats and vulnerabilities, and measure the effectiveness of existing controls and estimate the likelihood of the Threat and the impact to the organization in the following categories:

- Access Controls-Organizations ability to control access to assets based on business requirements and “need to know”.
- Asset Classification and Control-ability of the security infrastructure to protect organizational assets.
- Security Policy- Organizations’ Management Support, commitment and direction.
- Organizational Security-the need for a management framework that creates, sustains and manages the security infrastructure.
- Personnel Security-ability to mitigate risk inherent in human interactions
- Physical and Environmental Security-risk inherited to organizational premises.
- Communications and Operations Management-ability to ensure correct and secure operation of its assets.
- System Development and Maintenance-ability to ensure that appropriate information system security controls are both incorporated and maintained.
- Business Continuity Management-ability to counteract interruptions to normal operations.
- Compliance-ability to remain compliant with regulatory, statutory contractual and security requirements.
- Information Security Incident Management – how has the organization responded to security incidents and how have improvements been implemented.

FYI....

AaSys will be closed on Monday, Jan. 21, 2008 in observance of Dr. Martin Luther King Jr.’s Birthday.

Are there topics that you would like to have covered in future newsletters? We are always looking for topics of interest. We welcome all suggestions! To submit a topic, subscribe, or unsubscribe to our distribution list, please email Shama Renée-McIntosh at smcintosh@aasysgroup.com.