Internal Audit Committee of Brevard County, Florida

Information Technology
Risk Assessment
Public Report

Prepared By:
Internal Auditors of Brevard County
September 30, 2009

Table of Contents

September 30, 2009

The Audit Committee of
Brevard County, Florida
Viera, Florida 32940-6699

Pursuant to the approved internal audit plan, we hereby submit our internal audit report covering information technology (IT) risk assessment for Brevard County, Florida (the "County"). Through our knowledge and discussions with management, the certain IT systems were identified for an initial enterprise-wide risk assessment. This focused IT risk assessment was conducted by applying both a data security and business view of IT risk. The subject matter covered under this audit is confidential in nature, and thus specific details of any deficiencies are not disclosed to avoid the possibility of compromising County information and security. This exemption from Florida Statutes 119.07(1) and 286.001 and other laws and rules requiring public access or disclosure is addressed under Florida Statute 281.301, Security systems; records and meetings exempt from public access or disclosure. We will be presenting this public report to the Audit Committee at the next scheduled meeting and all confidential matters will be communicated with appropriate personnel at the County.

Our IT risk assessment methodology includes using National Institute of Science and Technology (NIST)[1] qualitative and quantitative risk assessment and other industry-accepted methodologies. Specifically, the risk assessment focuses on the data risk factors and effectiveness of Committee of Sponsoring Organizations (COSO) and Control Objectives for Information-related Technologies (CobIT) control framework elements employed to mitigate these data risks, as follows:

- Data risk elements (inherent risk in the absence of controls)
    - External market reputation
    - Operational/reliability and maintainability
    - Strategic
    - People/culture
    - Financial
    - Legal/regulatory
    - Technology/systems
    - Fraud
- Mitigating COSO-based controls (control design adequacy)
    - Monitoring
    - Risk assessment
    - Control environment—Tone at the Top
    - Information and communication
    - Control activities—preventive controls
- Residual risk (inherent risk—design adequacy of controls = residual risk)

While we obtained an understanding of the controls in place in order to assess the risks, our approach did not include testing the existing controls of these systems. To further enhance the value of this risk assessment process, the internal auditors facilitated key control identifications for these systems through the use of control self assessments (CSA's). This included documenting each of these systems' specific risks controls and performing transaction walkthroughs as appropriate to provide management with the process documentation needed for ongoing risk assessment and control design evaluation. We would like to thank the IT department, Planning and Zoning, Library Services, Utility Services, and Solid Waste Management in assisting with this IT risk assessment.

Sincerely,

INTERNAL AUDITORS

[1] NIST SPECIAL PUBLICATION 800-30, RISK MANAGEMENT GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS, DATED JULY 2002

Objectives and Scope

Objectives

Every entity faces a variety of risks from external and internal sources that must be assessed. Risk assessment is the identification and analysis of relevant risks to achievement of business objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change. Risk assessment should be performed as an on-going process.

The purpose of the Information Technology Risk Assessment was to assist management at the County with identifying and documenting the risks associated with critical applications to ensure there is a solid foundation for management to develop a strategy and operational plan for managing those risks. The performance of these risk assessments will facilitate not only the refinement and, if needed, development of key internal controls, but also enable the County to further establish a broad-based service-level management process based on specific risk criteria. As such, we will continue to include IT risk assessments in our proposed future internal audit plans.

A risk assessment does not include detailed testing of the controls in place. To further enhance the value of this risk assessment, we will be documenting each of these systems' specific risks and controls and performing transaction walkthroughs as appropriate to provide management with the process documentation needed for ongoing risk assessment and control design evaluation.

Scope

During the past year, the information technology department (ITD) has performed risk assessments for IT facilities, internet connections and 911 operations. In addition to these areas, management identified other high-risk IT systems that should be included in the initial enterprise-wide risk assessment of critical systems. In order to facilitate and assist management with the completion of the risk assessment, we planned the scope and extent of procedures based on County management's, as well as our own understanding of the criticality associated with the applications' data and business operations, and regulatory compliance. It should be noted the risk assessments are of the systems and/or applications and not necessarily the departments or agencies that use or develop them. Specifically, ITD identified that including the following systems or functions in the County's initial enterprise-wide risk assessment would bring the greatest benefit to the County's security program management process:

- Financial system - This application suite is the primary financial management and reporting application for the County. The system was the focus of a security review in 2008, with one remaining follow-up issue related to security policies.
- Permitting application - This application is the primary software utilized to track the approval process for permits, developments and contractor licenses. Additionally, it is used to track the enforcement process for code and contractor violations.
- Solid Waste Management Department (SWMD) application - SWMD is responsible for the operation of the County's landfills to provide for the disposal of solid waste that is generated from households and commercial businesses in Brevard County. SWMD will bill for collection and disposal charges for garbage, yard waste and recycling, as well as other services.
- Library Information Systems application - The Integrated Library Systems' (ILS) is used to manage library business.
- Utility Services application - This application is a complete work management system for Brevard County wastewater operations. It helps to automate the current manual processes and will support the management of work flow processes, assist with FEMA reporting, track and report DEP malfunction reports, and improve department accountability and efficiency. This system is currently in the design phase, and is scheduled to "go live" in February 2010.

Approach

Our approach consisted of the following phases:

Understand and Document the Risks

Our previous audit work over the last several annual internal audit plans has included obtaining an understanding of and documenting the processes and existing controls for the following IT areas at Brevard County:

- IT Planning and Organization Phase I
- IT Network Security Threat & Vulnerability Assessment
- Financial System Security

During these internal audits, we have also performed system and application testing and analyzed results, making recommendations for improvement and assisting management with determining cost efficient means of securing IT assets and data, as well as complying with various laws, policies and other regulatory requirements. These projects have provided our IT professionals with timely, relevant and specific knowledge of the County's IT infrastructure, hardware and software.

To assist management with application risk assessment, we conducted various interviews with senior management (operations and IT) and key technology and documentation management staff to discuss the specific objectives, scope and initial data requests needed to complete each phase of this risk assessment project.

Three types of risk were considered during this phase of the IT risk assessment: inherent, control and residual risk.

- *Inherent risk* the level of risk that a problem can occur without considering internal controls. Inherent risks apply to the activity itself, not the organization or its people.
- *Control risk* is the threat that errors or irregularities in the underlying transactions will not be prevented, detected and/or corrected by the internal controls in place. Defining control risk includes determining how well the control in place mitigates the inherent risk, as well as whether the control in place is operating as intended. (A risk assessment does not include detailed testing of the controls in place.)
- *Residual risk* is defined as the risk that a problem could occur after existing controls have been applied. Residual risk is entity-specific, taking the organization's control environment into consideration and can vary within an organization based upon management's risk-appetite over time. Residual risk can also be defined as the level of risk that management has deemed acceptable and/or appropriate for the organization, given current available resources.

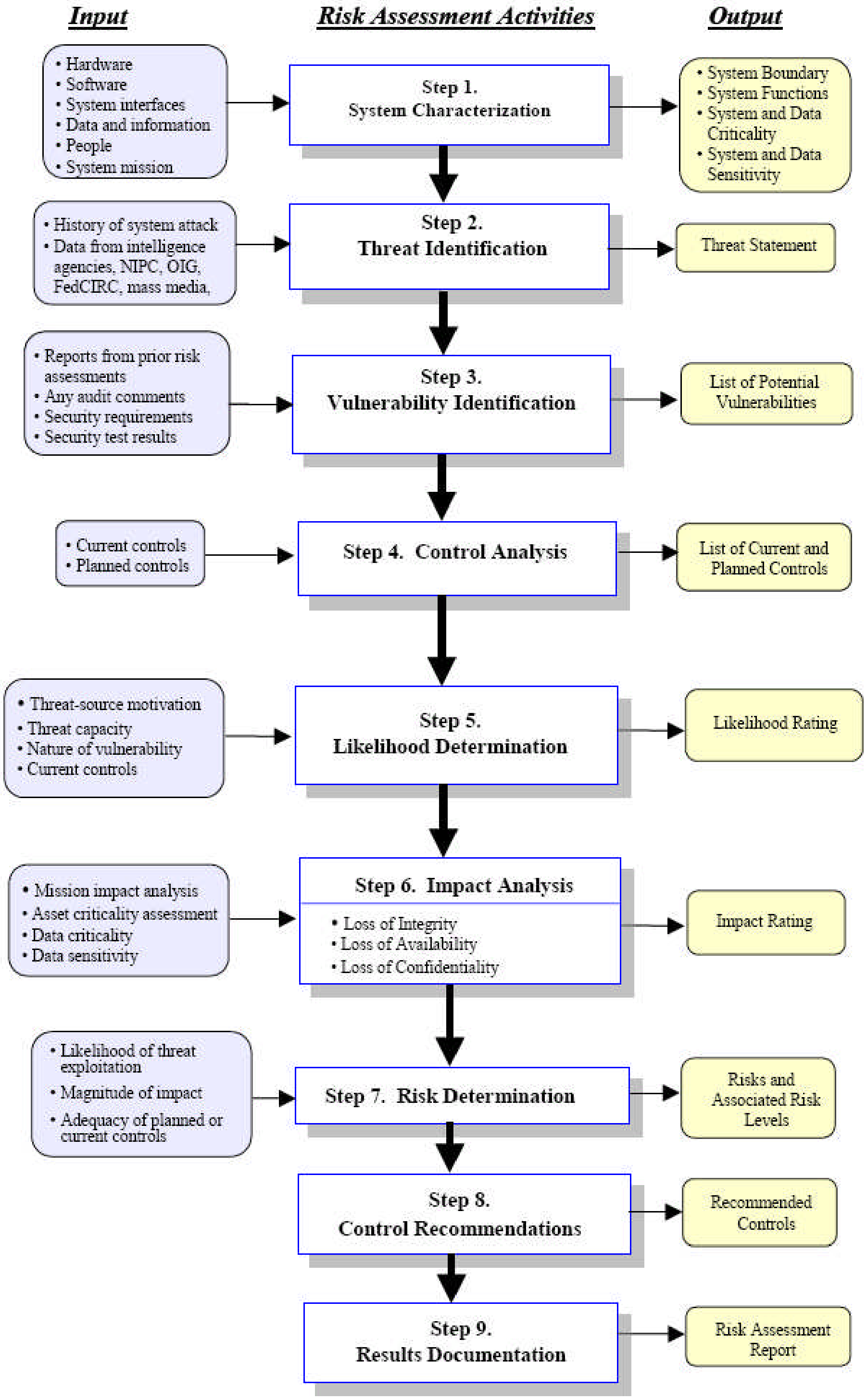
Based upon interviews and various analyses of these systems and functions, our IT assurance professionals documented the associated risks as described above.

The IT risk assessment process is illustrated on the following page.

Approach - continued

Understand and Document the Risks - continued

Information Technology Risk Assessment Activities



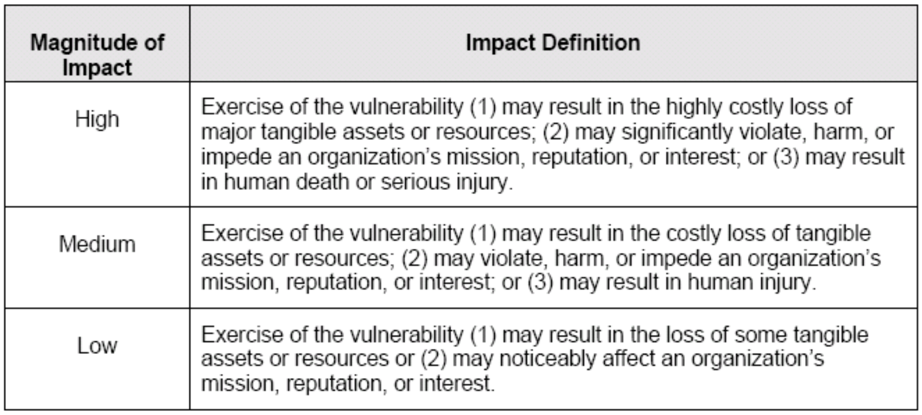
Approach - continued

Detailed Analysis

Management, with facilitation from our IT consultants, applied a three-step process for assigning risk factors, first determining the severity of the risks that apply to the environment without accounting for controls that may exist (inherent risk), understanding how existing controls mitigate the inherent risks identified (control risk), and then evaluating the level of risk that remains after controls have been applied (residual risk).

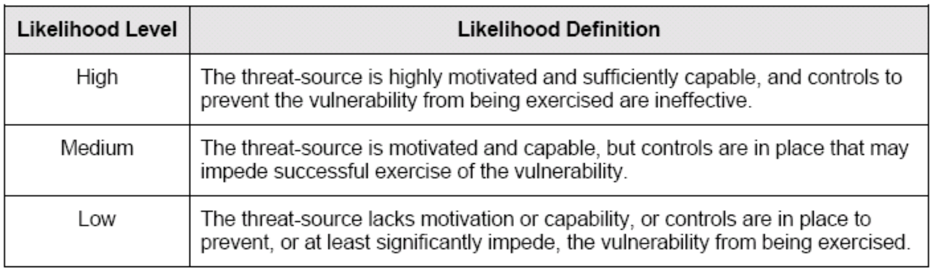
Risk factors were considered and evaluated on a scale of high, moderate or low (or weak, moderate, strong). The criteria used for evaluating each risk factor are shown below.

IMPACT CRITERIA



Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

LIKELIHOOD CRITERIA



Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Step One: Inherent Risk

Inherent risk is measured in terms of high, moderate, and low. The inherent risk factors used in this phase of our detailed analysis are defined as follows:

External Market Reputation - The risk of exposure related to fluctuations in the market value and marketability of an organization's assets. For the County, this is more accurately defined as public perception risk.

Financial - The risk that financial reporting is inaccurate, incomplete or untimely due to a variety of factors, including the pace of change, the amount of uncertainty, the presence of a large error, or the pressure on management to meet stakeholder expectations.

Operational - The organization provides or is reliant on outsiders to provide processing activities supporting the delivery of services to end users. This risk addresses barriers to the timeliness, accuracy, authorization and completeness of these processing activities.

Approach - continued

Detailed Analysis - continued

Step One: Inherent Risk - continued

Legal/Regulatory - The organization is subject to a variety of federal, state and local laws, regulations and directives. Failure to follow proscribed directives may result in substantial fines, restrictions in activities, and/or major concerns by regulators.

Strategic - The risk that business objectives will not be achieved because business strategies are poorly defined and communicated or the organization is unable to execute these strategies due to inadequate organizational structure, infrastructure or alignment. Strategic risk is managed by appropriate organizational governance. Failure to adequately plan and execute against organizational goals may result in significant damage to the organization's reputation.

Technology/Systems - This risk considers the level of use, sophistication, complexity, robustness, ease of use and speed and accuracy of recovery/replacement of systems. Addresses the overall importance of technology within the organization and the availability and quality of information the organization can access to support decision making, and the security around key information.

People/Culture - This risk addresses cultural factors in the organization such as the ethical tone of management, the type of behaviors encouraged by and methods of reward used in its incentive systems and the approach to and consistency of enforcement of policies and procedures in the organization. The length, consistency and nature of business relationships with vendors and customers, including the handling of sensitive or confidential information and the risk that business interruption would seriously impact those relationships is considered. Finally, the selection, screening and training of its employees, the complexity of the learning curve to perform the organization's work and the nature and pace of turnover are key factors in this risk.

Fraud - This risk addresses the structure of business activities and transaction processing and the organization's susceptibility to both internal and external fraud. The likelihood and ease of inappropriate management override as well as the timeliness, accuracy and completeness of fraud protection and monitoring activities should be considered. The nature (liquidity, value and access) of the products and assets of the business is critical to the assessment of fraud risk. Additionally, fraud risk incorporates intentional misstatement of financial reporting regardless of whether assets or products are misappropriated.

Step Two: Control Risk

Control risk is measured in terms of weak, moderate, and strong. The control risk factors used in this phase of our approach are defined as follows:

Control Environment - The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.

Risk Assessment - Every entity faces a variety of risks from external and internal sources that must be assessed. Risk assessment is the identification and analysis of relevant risks to achievement of business objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change. For each application or function rated at the County within this report, the control risk is rated as High (or weak controls) because risk assessment has not been previously performed. An ongoing risk assessment process should reduce the associated level of control risk.

Approach - continued

Detailed Analysis - continued

Step Two: Control Risk - continued

Control Activities - Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization at all levels and in all functions. They include activities such as segregation of duties, authorizations, security of assets, reporting and reviews of operating performance and documentation.

Information and Communication - Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports that make it possible to run and control the business. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive information needed to make informed business decisions.

Monitoring - Internal control systems need to be monitored. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. There is synergy and linage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise.

Step Three: Residual Risk

The Residual Risk rating shown in the illustrative heat maps on the following pages is a subjective evaluation of the severity of the concerns related to each application, given the controls in place and the likelihood of failure, as well as the potential impact on operations.

Residual risk is measured in terms of high, moderate and low. Items rated "High" are considered to be of immediate concern and could cause significant operational issues if proposed next steps are not addressed in a timely manner. Items rated "Moderate" may also cause operational issues and do not require immediate attention, but proposed next steps should be addressed as soon as possible. Items rated "Low" could escalate into operational issues, but can be addressed through the normal course of conducting business.

It should be noted that Residual Risk is not indicative of a security risk unless explicitly stated. Additionally, a risk assessment does not include detailed testing of the controls in place.

Reporting

Once documented, we conduct a formal exit conference with the appropriate management and support staff and discuss the results of the risk assessments and next steps that should be performed for each high risk application or function. While we obtain an understanding of the controls in place in order to assess the risks, our approach does not include testing the existing controls of these systems. To further enhance the value of this risk assessment process, we document each of these systems' specific risks controls and perform transaction walkthroughs as appropriate to provide management with the process documentation needed for ongoing risk assessment and control design evaluation. The confidential report contains a risk and control matrix for each application as well as an illustrated Heat Map to identify the risk areas.

Risk Assessment:

Financial System

This application suite is the primary financial management and reporting application for the County. Inherent risk – that is, the risk associated with the application without considering any controls that are in place - is assessed as "**High**" due to being the system of record for the finance-related activities of the County, as well as the significant number of transactions that flow through the system, and the nature of the transactions and information in the system. The system was the focus of a security review in 2008, with one remaining follow-up issue related to security policies.

The specific applications in use at the County include the following:

a. Logistics
   - Modules currently in use
     - Materials Management—Creating purchase requisitions and purchase orders
     - Plant Maintenance—Tracking facilities maintenance and work orders
   - Modules currently not in use
     - Customer Service—Tracking billing and contracts

b. Accounting – Financial Accounting
   - Modules currently in use
     - General Ledger—Daily financial transactions
     - Accounts Receivable—Billing for limited external agencies for various services
     - Accounts Payable
     - Banks—Payroll banks for employees
     - Fixed Assets—Asset management inventory
     - Special Purpose Ledger—Use for reporting, e.g., CAFR
   - Modules currently not in use
     - Lease Accounting—Accounting-relevant aspects of the leasing deal

c. Accounting – Treasury
   - Modules currently used
     - Controlling—Cost center information
     - Public Sector Management—Budget functions and availability control
   - Modules currently not in use
     - Investment Management—Enterprise project management
     - Real Estate Management—Management of property acquisition, disposal and portfolio management
     - Flexible Real Estate Management—Contract management and space management

d. Human Resources (All modules currently in use)
   - Personnel Management
   - Time Management
   - Payroll
   - Training and Event Management
   - Organizational Management—Departmental structure of the County

Analysis and Results Included in the Confidential Report

Risk Assessment:

Permitting Application

The permitting application is the primary software utilized to track the approval process for permits, developments and contractor licenses. Additionally, it is used to track the enforcement process for code and contractor violations. Inherent risk – that is, the risk associated with the application without considering any controls that are in place - has been assessed as "**Moderate**" due to being the mechanism for tracking permits, required reviews and associated fees, as well as interfacing with the financial system. This application could be "high" risk, but has been categorized at "moderate" given the reduced quantity of permits currently processed through the system.

The permitting application is composed of four modules that support wireless access:

a. Building Code
   - Building plan review and permitting (residential and commercial)
   - New construction inspection
   - Special event permitting
   - Bingo licensing
   - Address assignment
     - Street naming and renaming
     - Legal descriptions of property

b. Land Development
   - Site plan and subdivision review and approval
   - Unpaved roads, flag stem lots and easements
   - Right-of-way and easement permitting
   - Central cashier
   - Impact fees

c. Licensing
   - Contractor licensing certification and investigation
   - Investigation of unlicensed contractors

d. Code Enforcement
   - Investigate zoning and solid waste complaints.
   - Investigate immediate health and safety issues brought to their attention.
   - Assist citizens with compliance measures before resorting to prosecution.
   - Assist the public courteously and expeditiously with all matters related to code violations.
   - Refer other complaints to the proper agency for follow-up investigation, e.g., building, environmental health, natural resources, road and bridge, occupational license, signs, contractors, water and land development codes.

Analysis and Results Included in the Confidential Report

Risk Assessment:

Solid Waste Management (SWMD) Application

SWMD is responsible for the operation of the County's landfills to provide for the disposal of solid waste that is generated from households and commercial businesses in Brevard County. SWMD will bill for various services that include the following:

- Collection and disposal charges for garbage, yard waste and recycling: The collection charge only applies to residents in the unincorporated areas of the county (i.e., areas not within city limits) and the disposal charge applies to all residents and commercial activities. The collection and disposal charges are put on the annual tax bill under the non ad-valorem special assessments.
- Properties that have been issued a Certificate of Occupancy after October 1, will receive a prorated assessment for these services.

The inherent risk – that is, the risk associated with the application without considering any controls that are in place - is rated as "**High**" risk due to the process is decentralized (i.e., accounting function does not occur within finance department), as well as other factors.

Analysis and Results Included in the Confidential Report

Risk Assessment:

Library Information Systems Application

The Integrated Library Systems' (ILS) sole purpose is to manage library business. The main application modules allow patrons to:

- Borrow library materials
- Return library materials
- Track patron holds
- Request fines and fees

This application's inherent risk – that is, the risk associated with the application without considering any controls that are in place - is rated as "**Moderate**". There are no material financial transactions associated with ILS. However, it is used to track and monitor library assets and is relied upon by the public for services.

Analysis and Results Included in the Confidential Report

Risk Assessment:

Utility Services Work Management Application

The Utility Services application is a complete work management system for Brevard County wastewater operations that is currently under development. Once implemented, the application will help automate current manual processes and will support the management of work flow processes, assist with FEMA reporting, track and report DEP malfunction reports, and improve department accountability and efficiency. This system is currently in the design phase. Go live is scheduled in February 2010. Inherent risk – that is, the risk associated with the application without considering any controls that are in place **-** is rated as "**High**" for this application.

The Utility Services department is currently implementing the following modules:

- Asset Control—Used to input and track assets relating to:
  - Water
  - Plant
  - Sewer
- Work Management—Project and work order time entry and tracking
- Customer Service—Citizen relationship manager and service request
- Inventory Control—Used to track parts and inventory (limited functionality at this time) for:
  - Fleet
  - Trailers
  - Pumps
- Map Drawer—Mapping tool user interface to GIS and to engage work management
- GeoAdmin—Management interface tied to ARC IVIS (County's GIS software)

Analysis and Results Included in the Confidential Report