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 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, recommendations for improvement and assisting management with determining cost efficient means of securing assets and data, as well as complying with various laws, policies and other regulatory requirements. These have provided our IT professionals with timely, relevant and specific knowledge of the County's IT hardware and software.

To assist management with application risk assessment, we conducted various interviews with senior (operations and IT) and key technology and documentation management staff to discuss the specific 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

- *Inherent risk* the level of risk that a problem can occur without considering internal controls. Inherent 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 detected and/or corrected by the internal controls in place. Defining control risk includes determining well the control in place mitigates the inherent risk, as well as whether the control in place is operating 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 Residual risk is entity-specific, taking the organization's control environment into consideration and can within an organization based upon management's risk-appetite over time. Residual risk can also be as the level of risk that management has deemed acceptable and/or appropriate for the organization, current available resources.