Durham County Audit Department

Information Technology Control Self-Assessment

June 14, 2016

Richard Edwards
Internal Audit Director
rcedwards@dconc.gov

Internal Audit Department
200 E. Main Street, 4th Floor
Durham, NC 27701
(919) 560-0042
FAX: (919)560-0057

June 14, 2016

Mr. Wendell Davis,
County Manager

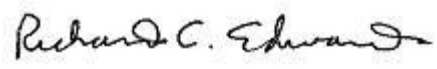
Dear Mr. Davis:

The Audit Committee has shown interest in Information Technology (IT) controls and requested an assessment of high-level risks that could affect continuation of IT activities.
The assessment is complete and attached to this memorandum.

The risk assessment does not require an audit conclusion or recommendations. However, risk assessments trigger audits under some circumstances such as the appearance of unreasonable ratings or unreasonable risk mitigation. A risk assessment is primarily a tool management uses to identify and lessen risks and provide a level of assurance that operations will continue if an adverse event was to occur.

Internal audit believes the risk assessment was well thought out by the IT team and provides meaningful information regarding the areas of threat it addressed.

Sincerely,



Richard Edwards,
Internal Audit Director

CC: Greg Marrow, IT Director
Audit Oversight Committee
Board of County Commissioner

Information Technology Risk Assessment

The Audit Oversight Committee is committed to continuous risk assessment of the County's Information Technology (IT) operations. In fiscal years 2014 and 2015, the Committee asked Internal Audit to conduct an assessment of IT's operational risks. Mr. Greg Marrow, the IT Director, addressed IT's security and continuity at the Committee's December 2015 and March 2016 Audit Oversight Committee meetings. The assessment below is the result of the latest efforts to identify IT's security and continuity risks from the viewpoint of the IT department.

IT used a "Control Self-Assessment" to assess its risks. In such a process, the operation identifies its risks and mitigating factors to lessen exposure to an adverse event. In this instance, Internal Audit developed the areas of assessment for IT to consider by brainstorming techniques. Additionally, Internal Audit researched and selected common areas assessed by IT practitioners and experts.

Purpose of Risk Assessment

The purpose of risk assessment is to assess and identify potential problems before they occur so managers can plan and invoke risk-handling activities to mitigate the risk of adverse impacts. Risk assessment is a component of risk management. Risk management is divided into three parts: defining a risk management strategy; identifying and analyzing risks; and handling identified risks, including the implementation of risk mitigation plans when needed. Risk management is a continuous, forward-looking process that is an important part of business and technical management processes. When conducted properly, management can use this tool to effectively anticipate and mitigate the risks that could potentially disrupt business operations. Additionally, early and aggressive detection of risk is important because advocates believe it is easier, less costly, and less disruptive to make changes and correct work efforts during the earlier phases of a project.

Options for Handling Identified Risks

When managers identify risks, they need to determine how best to manage them. The four main strategies are (1) avoid it, (2) reduce it, (3) transfer it, or (4) accept it. Each strategy has its own advantages and disadvantages, generally related to costs and resources. For example, it may sometimes be necessary to avoid a risk (the costlier option), or accept it (the least costly option), and other times the best option may be to reduce or transfer it. In reviewing IT's risks, it is apparent that some risks need to be closely watched because IT's environmental changes are sometimes rapid. The County's IT director appears cognizant of the rapid changes and exposures and keeps County employees aware through periodic emails and other communications. Internal Audit encourages continuation of efforts to remain current with risks and potential mitigating activity.

IT Assigned Ranges within Low to Moderate Risk Ratings

Internal Audit provided the rating scale IT used to determine its risks. We asked IT to estimate its risk by calculating a score by multiplying the probability of an event by the impact the event would have on its operations. For example, probability ranged from one to five with one being the least probability of an event occurring. Internal Audit designed the severity of impact to be judged by IT with the same range of possibilities. The probability multiplied by the impact resulted in the overall risk factor. An item could have a possible range of 1 to 25. (Please see the actual results of the risk assessment.)

IT assigned ranges that fell within the low to moderate risk ratings for all 41 of the items it assessed. Internal Audit did not attempt to determine if IT's ratings were representative nor did Internal Audit attempt to determine if the risk management strategy is adequate and competent. Internal audit's role was to assist, as necessary, in helping management identify its objectives. We believe the IT's management understands its objectives and the potential effects an adverse event would have on its operations.

Exhibit 1

Range	Rating	No. of items ranked
1-8	Low	35
9-16	Moderate	6
17-25	High	0
Total		41

Source: Information Technology Department Risk Assessment

IT posted the following general note to its risk assessment. "*Information technology has a backup and recovery system that stores data to tape off-site on a weekly schedule to a secure facility. A hot or warm redundant site (leased, County owned, or cloud services) is needed to improve the disaster recovery capabilities of the County in a timely manner to limit disruption of County business departments and services.*"

The IT Director said his team is currently evaluating alternatives for a warm site (cloud, leased, County owned, or City owned). He said the goal is to complete the evaluation by the end of December 2016.

Information Technology Risk Assessment

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
Flooding - Internal	2	2	**4**	*There is minimal threat of internal flooding damaging our systems. Data center cooling systems have a warning system to effect response. The most significant internal flooding threats are to the server rooms of the Health and Human Services building (also has a warning system in place) and the currently vacant facility at 201 East Main Street due to basement locations, underground conduits, and past experience. In addition, some aging facilities may incur plumbing issues in areas adjacent to technology closets.*
Flooding - External	2	3	**6**	*Facilities have not experienced an external flooding event and the core data-center is located on the 5th floor of the County Administration building. However, ground level access points in nearly all facilities provide communication services and flooding has potential impacts to those areas that would affect data and voice network communications and services.*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
Fire – Internal	1	5	**5**	*Buildings and datacenters have fire-extinguishing systems, hand-held extinguishers and personnel are trained to respond. However, the core datacenter is not staffed 24 hours each day of the week. Fire could potentially result in loss of significant technology resources.*
Fire - External	1	5	**5**	*An external fire from an adjacent building or the railway in close proximity to the property could potentially cause severe damage to the building and our core datacenter. See #3 above for mitigation.*
Severe Rain and Thunder Storms	2	3	**6**	*Facilities have not experienced issues in this regard and the core data-center is located on the 5th floor of the County Administration building. Associated loss of power is addressed in item #26 below.*
Wind Storm	2	3	**6**	*Although the roof over the core data center was replaced with a more resilient semi-translucent material, it may not stand to extremely high winds.*
Earthquake	1	5	**5**	*Risk of an earthquake in the area is low. Depending on the severity of a quake, the results could be significant.*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
Tornado	1	5	**5**	*Same as "Earthquake" response.*
Hurricane	2	5	**10**	*Same as "Earthquake" response*
Snow Storm	3	1	**3**	*Snow and related ice occur occasionally in the area to the point of closing business activities but actual threat to the operations or infrastructure is minimal.*
Hail	3	2	**6**	*Hail occurs occasionally but not of significant size to damage infrastructure. However, the roof over the datacenter is a semi-translucent material that may not withstand extremely large and dense hail if it were to occur.*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
Epidemic	1	3	**3**	*Experience, skills, and knowledge needed to support many of our systems would be impacted by time to respond and correct issues with reduced staff. This could affect the business operations of our departments. Staff are cross-trained in many areas but daily operational knowledge and experience are key to timely response and recovery. Business departments or support staff can do some work remotely.*
Pandemic	1	4	**4**	*See "Epidemic" response above; significant loss of staff or inability to access systems would cause greater impact to operations.*
Explosion	1	5	**5**	*See "Gas leak" response below: An external explosion depending on the location and size of the blast could have little to significant impact to County facilities.*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
Gas Leak - External	1	1	**1**	*A gas leak without an explosion may cause temporary interruption to operations depending on its size and location for the duration of incident but minimal lasting impact. Railway line adjacent to the building could be a potential source. An explosion, see #14 above*
Structural Failure e.g. Building Collapse	1	5	**5**	*Structural failure or loss of most county facilities can be recovered from a technology perspective within a few days if a suitable alternate facility is provided but there are no current predesignated facilities for this purpose for our facilities. The loss of the County Administration building housing the core of the network, and the County data center would be a huge, difficult, complex, and extended recovery due to the lack of any predetermined facility (cold-site) or a preferred alternate warm or hot site, which would have equipment at the ready. Several County applications are provided from cloud services and these can potentially be restored more quickly. For the past several years, our department has taken a cloud-first approach when planning new systems or migrations of older systems.*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
IT - System Software Failures	2	4	**8**	*System software is reviewed, patched and current to minimize failures; iSeries System is due for an upgrade. Obsolete and unsupported system software is replaced / removed in a timely manner.*
IT - Applications Failures	2	4	**8**	*Business applications are typically supported under maintenance agreements or in-house staff. Applications are moving to services in the cloud to better support business continuity and disaster recovery. Backups are taken routinely and stored securely off-site. For the past several years, our department has taken a cloud-first approach when planning new systems or migrations of older systems.*
IT - Hardware Failures	2	3	**6**	*Hardware failures are mitigated by several means including redundancies built into hardware components or secondary components and services depending on the criticality of the component or service. Virtualization of server systems has reduced hardware failure issues significantly.*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
IT Viruses	4	3	**12**	*Virus attacks are a known constant with multiple attack vectors. Mitigation is approached through multi-layered defenses from the network perimeter to our client systems, policy, employee training, and continuous awareness efforts. Increased use of mobile devices and limited mobile device management are a growing concern. Request for Mobile Device Management system and polices are in process. Recently upgraded our security with the deployment of advanced threat protection capabilities in the firewall.*
Hacking, Unauthorized Intrusions	3	5	**15**	*Intrusions into our environment are a known constant threat with multi attack vectors. Mitigation is approached through multi-layered defenses from the network perimeter to our client systems, policy, employee training, and awareness efforts. Recently upgraded our security with the deployment of advanced threat protection capabilities in the firewall. Also currently in process is an RFP for monitoring services to aid in the firewall traffic analysis that will detect and mitigate threats proactively.*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact.	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
Communications, Connectivity Failures	2	5	**10**	*Although we have not experienced a significant communications failure potential for malicious acts or significant wide spread ISP failures remain a cyber security concern. Addition of a secondary ISP and our internal fiber ring supporting a dozen and most of our larger facilities may mitigate impact.*
Vendor Failure	3	5	**15**	*The County has many vendors supplying critical services and support for significant business operations. Common services and equipment have multiple vendor sources. Use of State contracts adds stability to vendor management due to the larger scale. Review and analysis of vendor management is needed.*
Operational (Human) Errors	2	3	**6**	*Numerous key personnel with access have the potential to error in critical systems. Most errors would be insignificant or recoverable from. See note below.*
Utilities - Water Shortages or Issues	1	1	**1**	*In recent history, North Carolina has been under drought conditions for several years without business impact.*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact.	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
Utilities - Sewage issues	1	1	**1**	*No history of sewage issues locally. County operates a waste treatment plant.*
Utilities - Electricity Failures	1	2	**2**	*Power failures are typically associated with winter storms and infrequently other causes. The critical data centers and systems have battery and generator power to sustain power if lost. Even if those systems failed, experience has shown we can recover. See note below.*
Terrorism - Biological	1	5	**5**	*As a government organization, the County would be a potential soft target. The number of terrorist attacks has sharply increased; in the United States terrorism risk remain low. However, damage from an attack could be significant.*
Terrorism - Chemical	1	5	**5**	*Same "Biological Terrorism"*
Terrorism - Radiological	1	5	**5**	*Same "Biological Terrorism"*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact.	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
Terrorism - Nuclear	1	5	**5**	*Same "Biological Terrorism"*
Sabotage	1	5	**5**	*As a government organization, the County would be a potential target. Impact could be significant if the data center was breached and damaged. Damage from internal sabotage could be significant. Background checks on staff is a standard part of hiring process. See note below.*
Bomb Threat	2	1	**2**	*As a government organization, the County is a potential target. Impact would be interruption of business activities. Standard training and processes are in place to protect staff and bring law enforcement resources to locate and neutralize threats.*
Criminal - Theft	1	2	**2**	*Limited instances / impacts in regards to technology. Badge security access is employed for critical areas. Many of the County facilities also have video surveillance systems and security officers.*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact.	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
Criminal - Break-ins	1	2	**2**	*No known instances / impacts in regards to technology. Badge security access is employed for critical areas. Many of the County facilities also have video surveillance systems and security officers.*
Criminal - Vandalism	1	5	**5**	*No known instances / impacts in regards to technology. Badge security access is employed for critical areas. Many of the County facilities also have video surveillance systems and security officers.*
Criminal - Espionage	2	1	**2**	*Low threat but our ability to access state and federal systems make us a potential avenue for hackers. Our systems would likely suffer collateral compromise or damage. Steps taken to mitigate hackers and viruses mentioned above and the background security checks of employees also mitigate concerns in this area*
Criminal - Hostages	1	1	**1**	*As a government organization, the County would be a potential target. Training for county employees mitigates impact as well as security officers and video surveillance.*

Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	Impact (I) The severity of the effect if the event was to occur. Rate 1 to 5 with 1 being the least impact.	Risk = P x I Risk score	Comments/Rationale Please explain mitigating factors relating to the risks.
Criminal - Murder, Rape, Assault	1	2	**2**	*Potential loss of staff, staff productivity. Badge access, security officers, and video surveillance systems are employed.*
Criminal - Bribery	1	4	**4**	*Potential compromise of financial, tax or confidential information, and resulting loss of funds and associated costs. Background security checks of employees also mitigate concerns in this area.*
Civil Disorder	2	5	**10**	*As a government organization, the County would be a potential target. Impact could be significant if the data center was breached and damaged. Training for county employees mitigates impact as well as security officers and video surveillance.*
GENERAL NOTE				*Information technology has a backup and recovery system that stores data to tape off-site on a weekly schedule to a secure facility. A hot or warm redundant site (leased, County owned, or cloud services) is needed to improve the disaster recovery capabilities of the County in a timely manner to limit disruption of County business departments and services.*