Durham County Internal Audit Department

Fourth Annual Information Services and Technology Control Self-Assessment

August 14, 2017

Kierra Simmons
Interim Internal Audit Director
ksimmons@dconc.gov

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

August 14, 2017

Mr. Wendell Davis,
County Manager

Dear Mr. Davis:

Internal Audit has requested IS&T to conduct its Annual Control-Self Assessment in an effort to keep Internal Audit and the Audit Oversight Committee apprised of its risk environment. The assessment is completed 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 this risk assessment provides meaningful information regarding the threats IS&T faces in securing Durham County's data and information that is transmitted, processed, accessed, and stored on mobile devices.

Sincerely,

Kierra Simmons, Esq.
Interim Internal Audit Director

CC: Greg Marrow, IS&T Director
Audit Oversight Committee
Board of County Commissioners

FOURTH ANNUAL INFORMATION SERVICES AND TECHNOLOGY RISK ASSESSMENT

The Audit Oversight Committee is committed to identifying and evaluating Durham County's information security risks. It believes continuous risk assessments of the County's Information Services and Technology (IS&T) operations is a vital tool in the County's overall internal control system. Beginning in 2015, IS&T has performed an annual risk assessment at the request of the Audit Oversight Committee in conjunction with the Internal Audit Department. IS&T uses a "Control Self-Assessment" to assess its risks on behalf of the Committee. In the process used by Internal Audit, Internal Audit identifies risks and IS&T reviews and rates them in terms of level (low, medium, of high), and provides mitigating factors that lessen the likelihood and impact if such an event occurred.

Purpose of Risk Management and Assessment

The purpose of risk management and assessment is to assess and identify potential problems before they occur so managers can plan and implement risk-mitigating activities. Risk management is divided into three parts: defining a risk management strategy; identifying and analyzing risks; and managing identified risks, including the implementation of risk mitigation plans as needed. Risk management is a continuous, forward-looking process that is an important part of business 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 to correct work efforts during the earlier phases of a project.

Options for Managing Risks

When management identifies risks, it needs to determine how best to manage them. The four main strategies are (1) avoid them, (2) reduce them, (3) transfer them, or (4) accept them. 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. According to risk management experts, management is responsible for making decisions regarding how it wants to manage risks. Internal audit's role is to provide assurance to management that the risk management processes are working effectively and that the key risks are being managed to an acceptable level.

IS&T rated its risks as low

Out of the 30 threats Internal Audit identified and asked IS&T to rate, the assessor rated the 23 threats as low risks. Internal Audit did not attempt to determine if IS&T's ratings were reasonable nor did Internal Audit attempt to determine if the risk management strategy is

adequate and competent. The following exhibit summarizes the frequency of ratings assigned by IS&T for the thirty risks Internal Audit identified.

Exhibit 1
IS&T Risk Rating for thirty risks

Risk Score Range	Rating	No. of risks ranked
1-8	Low	23
9-16	Moderate	7
17-25	High	0
Total Comments		30

Source: IS&T Risk Assessment

IS&T has developed a policy and mobile device management system to address risks

Many of Durham County's employees use mobile devices—e.g., cellphones, smartphones, laptops, and tablet computers—on a daily basis to communicate, obtain internet-based information, access data, and share information. Given the extent of reliance on mobile interactions, it is increasingly important that these devices be secured from expanding threats to the confidentiality, integrity, and availability of the information they maintain and share. Threats to the security of mobile devices and the information they store and process have been increasing significantly.[1] These threats and attacks are facilitated by vulnerabilities in the design and configuration of mobile devices, as well as the ways consumers use them.[2] In an effort to address threats and govern the usage of mobile devices, IS&T has developed a draft policy for mobile devices that is awaiting formal approval. Once approved, the department will distribute the policy throughout the County, by department, and launch the new Mobile Device Management System that will provide a layer of protection for information accessed and processed on employees' personal mobile devices.

[1] U.S. Government Accountability Office. *INFORMATION SECURITY: Better Implementation of Controls for Mobile Devices Should Be Encouraged*. GAO-12-757: Published: Sep 18, 2012. Publicly Released: Sep 18, 2012.
[2] See footnote 1.

ANNUAL INFORMATION SERVICES AND 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 threats.
1	**Lack of an official Mobile Device Security Policy**	2	3	6	A mobile device management policy is in draft awaiting review and signature. Our operational practice has positive impact on mobile security.
2	**Inadequate policies and procedures to address screenshots and camera use**	2	3	6	A mobile device management policy is in draft awaiting review and signature. Our operational practice has positive impact on mobile security.
3	**Insufficient employee training and education about mobile device security risks**	2	3	6	Significant Security Awareness Training was provided last FY including phishing exercises and strong focus during Cyber Security Month. Currently a security training program is being planned by the new Information Security Officer.

	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 threats.
4	**Employees are unaware of which outdated devices/operating systems pose significant security risks**	2	3	6	County devices are maintained currently. Personal devices (smartphones) will come in under the new mobile device management tool.
5	**Employees failing to maintain the software configurations of the mobile devices**	2	3	6	County laptops / tablets are kept current through management tools. Personal devices and smartphones will be managed under the new mobile device management tool that is currently being deployed. Once deployed devices not meeting security criteria will not be allowed connection to the network.
6	**Employees intermingle County data and personal data**	2	3	6	This will be restricted by policy in development. No past or current issues at this time. Also new MDM tool will segregate County data from personal data to further restrict but not eliminate this.

	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 threats.
7	**Inadequate layered password protection when accessing County data using mobile devices**	3	3	9	Requirement for password on county access and policy requirement for a PIN. Will be enforced with MDM being deployed.
8	**Lack of controls to prevent unauthorized access to data through the use of browser saved passwords**	2	3	6	Current practice requires individuals to authenticate through Active Directory. Saved passwords would be restricted to the authenticated user. Means to restrict this capability further are being reviewed.
9	**Decryption of files or data**	1	5	5	County laptops being encrypted; currently 80-plus percent are encrypted. Under new MDM tools data on mobile devices will be encrypted. Datacenter drives are encrypted. Current technologies are deployed aligned with best practices to mitigate decryption.

	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 threats.
10	**Lack of encryption on wireless transmissions (i.e., emails, email attachments)**	1	5	5	Commercial carrier and County wireless transmissions are encrypted in alignment with best practices.
11	**Inadequate malware prevention software for mobile devices**	3	3	9	Mobile devices using county approved applications are only used to access DCG information. The approved applications are patched and upgraded as they are available. Data will be located within the cloud or IS&T data center which is scanned on a regular basis to minimize exposure to malware.
12	**Malware attacks or unauthorized eavesdropping through open Bluetooth connections**	1	5	5	Advanced skills and tools required as well as social engineering for user interaction minimize risks.

	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 threats.
13	**Insufficient controls to identify when data security is compromised on mobile devices**	3	3	9	Limit data on mobile devices. Increased security in coming MDM. Most County Laptops are encrypted. County approved applications are only used for access to county resources. Users are required to notify if the device is lost or compromised immediately once they become aware.
14	**Inadequate disabling process of County applications when mobile device security is compromised**	1	5	5	Authentication accounts can be turned off when notified. Policy will require notification.
15	**Insufficient restrictions on applications that can be installed on mobile devices**	1	5	5	County applications will be separated and secured from personal applications and data under mobile device management.
16	**Lack of procedures to safely dispose of old or broken mobile devices which contain County data**	1	2	2	County data on mobile devices will be encrypted. Minimal data is on mobile devices; data is usually stored in cloud services and further secured.

	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 threats.
17	**Lack of procedures to prevent data from being stored on mobile devices indefinitely**	1	2	2	County data on mobile devices will be encrypted. Minimal data is on mobile devices; data is usually stored in cloud services and further secured. The MDM solution will prevent county data from being stored locally.
18	**Inadequate controls (i.e., training, education, and firewall) to ensure personnel is not subject to Network spoofing**	2	3	6	The County employs state-of-the-art firewalls and managed security services to mitigate network spoofing. User education is given annually and reminders are communicated monthly.
19	**Unsecured Wi-Fi use**	2	3	6	County wireless networks are secured to minimize in the work place. User education has been provided and continual awareness will be focus of the new CISO.

	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 threats.
20	**Hackers attacking the infrastructure through the server, routers, and network access providers.**	3	5	15	The County employs state-of-the-art firewalls, managed security services, a layered security model, has associations with multi-state and national cyber security agencies and other tools to mitigate. But government agencies remain a significant target.
21	**Unauthorized access to data by former employees who have remote access to the County network**	1	1	1	Former employees' access to County data is removed when employees are terminated. Troublesome terminations are handled promptly.
22	**Insufficient security to protect against attacks through screen sharing and remote administration software weaknesses**	1	3	3	Sharing is typically with trusted and known personnel. Impact of remote administration is limited to the level of the user.
23	**Public disclosure of sensitive data/Data leakage**	2	5	10	Employees within the various departments have access to sensitive data and those departments enforce the handling of that data through policy and procedures.

	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 threats.
24	**Inadvertent loss of data (i.e., personnel accidentally wipes out data or loses device)**	1	2	2	Data is to be stored in cloud services or networked drives; is backed up and recoverable in most cases.
25	**Loss of data due to hostile threats (i.e., theft)**	2	5	10	External threats are addressed by the County employed state-of-the-art firewalls, managed security services, a layered security model, associations with multi-state and national cyber security agencies and other tools to mitigate. Internal threats today are managed through policy and procedures within each department in terms of handling of data. But government agencies remain a significant target.
26	**Lack of inventory of County issued/owned devices**	2	5	10	An inventory of County devices is maintained by the client services and support manager.
27	**Lack of procedures to back up data stored on mobile devices**	1	1	1	Most County data is recoverable from cloud 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 threats.
28	**Lack of disaster recovery plan that extends to mobile devices**	1	2	2	Mobile devices can be easily replaced and accounts for access to resources reestablished.
29	**Lack of security software/controls to prevent sensitive data from being copied**	1	3	3	SAME AS QUESTION #2 ABOVE
30	**Lack of controls to address unauthorized modifications (i.e., Jailbreaking, rooting) on mobile devices**	1	2	2	Written policy in draft and new MDM will not allow.