Durham County Internal Audit Department

Information Systems and Technology Control Self-Assessment

December 9, 2021

Darlana Moore
Internal Audit Director
damorre@dconc.gov

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

December 9, 2021

Ms. Claudia Hager,
Interim County
Manager

Dear Ms. Hager:

Internal Audit has requested IS&T to conduct its Control Self-Assessment 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 county devices.

Sincerely,

Darlana M. Moore

Darlana M. Moore
Internal Audit Director

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

IS&T Control Risk Assessment

The Audit Oversight Committee is committed to identifying and evaluating Durham County's information security risks. It believes continuous risk assessments of IS&T operations is a vital tool in the County's overall internal control system. IS&T used 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 48 threats Internal Audit identified and asked IS&T to rate, the assessor rated 35 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 forty-eight risks Internal Audit identified.

Exhibit 1
IS&T Risk Rating

Risk Score Range	Rating	No. of risks ranked
1-8	Low	35
9-16	Moderate	11
17-25	High	2
Total Comments		48

Source: IS&T Risk Assessment

IS&T Risk Assessment					
Threat #	**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	1	1	1	All county users are still under the governance of the Acceptable Use Policy as well as the Mobile Device Security Policy.
2	Inadequate policies and procedures to address screenshots and camera use	1	1	1	All county users are still under the governance of the Acceptable Use Policy even if there is not a Mobile Device Security Policy available. In addition, the information captured on county owned devices belong to the county.
3	Insufficient employee training and education about mobile device security risks	1	1	1	All county employees receive annual security awareness training. In addition, occasional training is done throughout the year via IS&T News Flash.
4	Employees are unaware of which outdated devices/operating systems pose significant security risks	3	1	3	Vulnerability Management is managed by IS&T. Mobile devices are update leveraging the Mobile Device Management (MDM) solution. Employees are frequently reminded to keep their devices on to ensure they are updated in a timely manner.
5	Employees failing to maintain the software configurations of the mobile devices	2	1	2	Software configurations are not permitted by user. This is managed by IS&T via the MDM solution.

Threat #	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.
6	Employees intermingle County data and personal data	3	1	3	If employees are using county devices, there is no expectation of privacy. This statement is provided when logging into Durham County laptops and desktops.
7	Inadequate layered password protection when accessing County data using mobile devices	1	1	1	Durham county network access is configured using conditional access. Therefore, users accessing county data via mobile device are required to use Multi-Factor Authentication (MFA) if outside of the county network.
8	Lack of controls to prevent unauthorized access to data using browser saved passwords	1	1	1	Cloud based applications that are integrated with the county Active Directory (AD) are required to MFA. Some cloud-based applications do not integrate.
9	Decryption of files or data	1	1	1	All end user devices are encrypted with either Intune/bit locker or the MDM solution
10	Lack of encryption on wireless transmissions (i.e., emails, email attachments)	1	1	1	Email is hosted with a cloud service. To access this service, the website is encrypted. Therefore, the communications are encrypted. In addition, email could encrypt emails.

Threat #	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.
11	Inadequate malware prevention software for mobile devices	1	1	1	County owned mobile devices are Apple devices, which applications are vetted prior to going into the Apple store. In addition, users cannot install applications outside of what is provided in the Company Portal. User cannot access the App Store.
12	Malware attacks or unauthorized eavesdropping through open Bluetooth connections	1	1	1	Bluetooth is not disabled. However, in order to complete the connection, pairing has to take place. This will not occur without user interaction.
13	Insufficient controls to identify when data security is compromised on mobile devices	2	1	2	MDM can control data on mobile devices. IS&T has not received any alerts for compromised accounts. We can kill a phone at any time if need it is required.
14	Inadequate disabling process of County applications when mobile device security is compromised	1	1	1	MDM allows us to kill a phone remotely if it has been compromised - if we are alerted by user to the compromise.
15	Insufficient restrictions on applications that can be installed on mobile devices	1	1	1	County owned mobile devices are Apple devices, which applications are vetted prior to going into the Apple store. In addition, users cannot install applications outside of what is provided in the Company Portal. User cannot access the App Store.
16	Lack of procedures to safely dispose of old or broken mobile devices which contain County data	1	3	3	all retired phones are returned to the vendor

Threat #	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	1	1	The MDM solution can control data storage.
18	Inadequate controls (i.e., training, education, and firewall) to ensure personnel is not subject to Network spoofing	2	1	2	other than cyber security training there is no training for mobile devices and no firewall on mobile devices.
19	Unsecured Wi-Fi use	5	3	15	Phones are allowed to connect to unsecure Wi-Fi.
20	Hackers attacking the infrastructure through the server, routers, and network access providers.	3	5	15	There is no such thing as a silver bullet for security. This risk will always be present. IS&T has implemented several infrastructure changes to include MFA for privileged accounts.
21	Unauthorized access to data by former employees who have remote access to the County network	3	4	12	Remote access to the County network is managed through AD. Once HR is notified of an employee leaving the county, the account is disabled, and the employee cannot longer access the network.
22	Insufficient security to protect against attacks through screen sharing and remote administration software weaknesses	1	1	1	IS&T does not allow remote administration tools to be installed on county devices outside of what the county uses. The county technical person will set up a remote session and monitor the activities of the remote resource.
23	Public disclosure of sensitive data/Data leakage	2	5	10	Data in IS&T systems are encrypted to include databases, laptops, and storage.

Threat #	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 wipe out data or loses device)	1	2	2	Durham county IT systems are continuously backed up and can be recovered. Employees using laptops and desktops are encouraged to store their information on OneDrive or the Shared Drive to ensure they are backed up.
25	Loss of data due to hostile threats (i.e., theft)	1	1	1	All laptops have hard drives and system databases encrypted and backed up to mitigate data loss. In addition, the backed-up information is stored off site.
26	Exposure when accessing County network from external locations and external devices (i.e., Starbucks or computers at public locations).	1	5	5	Employees requiring access to the county network are required to use the Virtual Private Network (VPN), which requires MFA.
27	Lack of inventory of County issued/owned devices.	4	5	20	IS&T uses the IT Service Management (ITSM) system to record IT assets before they are given to the user. IS&T is beginning the implementation of a new ITSM to add additional capabilities to tracking assets.
28	Lack of procedures to back up data stored on mobile devices.	1	1	1	Mobile devices are used to access information. Critical information will not be stored on the device. In addition, text messages are captured by the MDM solution.

Threat #	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.
29	Lack of disaster recovery plan that extends to mobile devices.	1	1	1	Critical business data is not stored on mobile devices.
30	Lack of security software/controls to prevent sensitive data from being copied.	3	5	15	IS&T is implementing a solution to identify sensitive data. This process is to help identify who has access to this information.
31	Lack of controls to address unauthorized modifications (i.e., Jailbreaking, rooting) on mobile devices.	1	1	1	County mobile devices will not operate as a county device if it is Jailbroken, based on our MDM policy. In addition, this is also in violation of the Acceptable Use Policy.
32	Undetected technical vulnerability such as a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation.	3	5	15	IS&T patches critical and high-risk vulnerabilities on a monthly basis after testing with various users across the county.
33	Vulnerabilities from interdependent and interconnected systems through relationships with third parties. Over time, as these systems become increasingly interdependent and complex, new vulnerabilities may be introduced, including those found in hardware and software products.	3	5	15	Durham county has some apps that are integrated with third-party cloud solutions. Most external apps IS&T requested to have Active Directory Integration. IS&T does leverage third party external risk service provided by the state to help identify potential gaps.

Threat #	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.
34	Threats from internal events from human errors, misconduct, and insider attacks affecting IT, as well as external events such as the County's ability to meet its operating objectives during and after natural disasters, cyber-attacks, new technologies, litigation, and new laws or regulations.	1	5	5	Durham County has a third-party monitoring the security of our environment 24/7/365. This service keeps the IS&T informed of malicious activities and vulnerabilities.
35	Users granted access to systems, applications, and databases, including elevated or administrator privileges and third-party vendors, not based on their job responsibilities.	2	5	10	Durham county system administrators use separate accounts to perform administrative functions. These accounts are limited to those performing these functions.
36	Lack of Network protections that have secure boundaries, and identification of "trusted" and "untrusted" zones.	1	3	3	Durham county has segmented its environment into multiple domains - systems and user. In addition, IS&T has started a project to perform segmentation of departments.
37	Lack of training to support security awareness and strengthen compliance with security and acceptable use policies.	1	2	2	Durham county requires annual security awareness training to include acknowledgment of IT policies, which includes the Acceptable Use Policy.
38	Lack of training materials that focus on issues such as end-point security, log-in requirements, and password administration guidelines.	3	1	3	IS&T provides occasional training via the IS&T News Flash. In addition, employees are required to acknowledge the IT policies.

Threat #	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.
39	Physical access and damage or destruction to physical components can impair the confidentiality, integrity, and availability of information.	1	3	3	Physical access to the data center is limited to employees that require access as part of their duties.
40	Because the user is not physically connected to the network and the wireless signal is broadcast and available to others, wireless networks are inherently less secure than wired networks.	5	2	10	Wireless connections could be vulnerable to multiple threats. However, wired connections could cause compromises as well. Therefore, all laptops have next-generation malware protection installed.
41	Malicious insiders and attackers may set up rogue or unauthorized wireless access points and trick employees into connecting. Such access points allow attackers to monitor employee activities.	1	1	1	County owned devices are setup to automatically connect to the county employee network. The employee would have to intentionally try to connect to another network.
42	Providing remote network connectivity for employees or third-party service providers who are not located within or around the County facilities presents a threat.	5	2	10	Third parties requiring access to IT systems remotely require IS&T to provide connections and be watched as they are making changes to the systems.
43	Lack of a process to introduce application and system changes, including hardware, software, and network devices, into the IT environment.	1	2	2	Durham county IS&T has an established Change Management process before anything would be put in production.

44	Lack of policies and procedures to ensure compliance with minimally acceptable system configuration requirements.	3	1	3	Durham county IS&T has an established Change Management process before anything would be put in production.
45	Lack of identification of unnecessary software and services increases the potential number of discovered and undiscovered vulnerabilities in a system.	5	5	25	IS&T is in the early stages of planning for an IT Asset Management tool to obtain all software and hardware assets which would bring more visibility to reduce the likelihood of having unpatched software in the environment.
46	Lack of penetration test that targets systems and users to identify weaknesses in business processes and technical controls.	1	2	2	Durham county IS&T performs annual penetration testing to help identify vulnerabilities.
47	Lack of a process that defines, identifies, and classifies the vulnerabilities in a computer, network, or communications infrastructure.	3	4	12	Durham county has Vulnerability Management tools to identify vulnerabilities in the computing environment.
48	Lack of a business continuity planning process that involves the recovery, resumption, and maintenance of the entire business, including outsourced activities.	1	3	3	IS&T has a Business Continuity Plan established for the department.