Durham County Internal Audit Department

Office of the Sheriff Technology Control Self-Assessment

December 10, 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 10, 2021

Ms. Claudia Hager,
Interim County Manager

Dear Ms. Hager:

Internal Audit has requested the Technology Communications department of the Sheriff's Office to conduct its Annual 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 the Technology department of the Office of the Sheriff (OOS) faces in securing Durham County's data and information that is transmitted, processed, accessed, and stored on county devices.

Sincerely,

Darlana Moore

Internal Audit Director

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

Office of the Sheriff Technology 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 the Sheriff's Office Technology Communications operations is a vital tool in the County's overall internal control system. Technology Communications 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 the OOS Technology department 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.

OOS Technology rated its risks as low and moderate

Out of the 48 threats Internal Audit identified and asked OOS Technology to rate, the assessor rated 21 threats as low risks and 22 threats as moderate risks. Internal Audit did not attempt to determine if the OOS Technology department'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 assignedby OOS Technology for the forty-eight risks Internal Audit identified.

Exhibit 1
OOS Technology Department Risk Rating

Risk Score Range	Rating	No. of risks ranked
1-8	Low	21
9-16	Moderate	22
17-25	High	5
Total Comments		48

Source: OOS Technology Risk Assessment

OOS Technology 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 OOS 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 OOS 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 OOS owned devices belong to the OOS.
3	Insufficient employee training and education about mobile device security risks	1	1	1	All OOS 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	2	1	2	Vulnerability Management will be managed by OOS IT. Mobile devices will be updated leveraging the Mobile Device Management (MDM) solution.
5	Employees failing to maintain the software configurations of the mobile devices	2	1	2	Software changes will not be permitted by user. This will be managed by OOS IT via the MDM solution.
6	Employees intermingle County data and personal data	3	1	3	If employees are using OOS devices, there is no expectation of privacy.
7	Inadequate layered password protection when accessing County data using mobile devices	1	1	1	OOS network access is configured using conditional access. Therefore, users accessing OOS data via mobile device are required to use Multi-Factor Authentication (MFA) if outside of the OOS network.

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.
8	Lack of controls to prevent unauthorized access to data through the use of browser saved passwords	1	1	1	Users that access data on the OOS network are required to use MFA.
9	Decryption of files or data	1	3	3	All end user devices will be 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 can encrypt emails.
11	Inadequate malware prevention software for mobile devices	3	1	3	OOS owned mobile devices are Apple devices, which applications will be vetted prior to going into the Apple store. In addition, users will not be able to 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, to complete the connection, pairing must 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 will control data on mobile devices. OOS will be able to kill a phone at any time if need is required.
14	Inadequate disabling process of County applications when mobile device security is compromised	2	2	4	MDM will allow us to kill a phone remotely if it has been compromised – If OOS IT is alerted by the user to the compromise

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.
15	Insufficient restrictions on applications that can be installed on mobile devices	1	1	1	OOS owned mobile devices are Apple devices, which applications will be vetted prior to going into the Apple store. In addition, users will not be able to install applications outside of what is provided in the Company Portal. User will not have access to 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
17	Lack of procedures to prevent data from being stored on mobile devices indefinitely	1	1	1	The MDM solution will control OOS 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	4	5	20	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	This risk will always be present. OOS IT has implemented several infrastructure changes to include MFA for privileged accounts.

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.
21	Unauthorized access to data by former employees who have remote access to the County network	3	5	15	Remote access to the OOS network is managed through AD. Once HR is notified of an employee leaving the OOS, the account is disabled, and the employee can no longer access the network.
22	Insufficient security to protect against attacks through screen sharing and remote administration software weaknesses	1	1	1	IT does not allow remote administration tools to be installed on our devices outside of what the OOS IT uses. The OOS 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 OOS systems are encrypted to include databases, laptops, and storage.
24	Inadvertent loss of data (i.e., personnel accidentally wipe out data or loses device)	1	1	1	The OOS data systems are continuously backed up and can be recovered. Employees using laptops and desktops are encouraged to store information on the Shared Drive.
25	Loss of data due to hostile threats (i.e., theft)	2	2	4	All system databases are backed up to mitigate data loss and users are instructed not to store data locally. 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)	2	5	10	Employees requiring access to the OOS network are required to use the Virtual Private Network (VPN), which requires MFA.

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.
27	Lack of inventory of County issued/owned devices	3	3	9	OOS uses the IT Service Management (ITSM) system to record IT assets before they are given to the user.
28	Lack of procedures to back up data stored on mobile devices	2	2	4	Mobile devices are used to access information. Critical information will not be stored on the device. In addition, text messages will be captured by the MDM solution.
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	2	2	4	OOS implemented a process that only allows approved users to access sensitive data.
31	Lack of controls to address unauthorized modifications (i.e., Jailbreaking, rooting) on mobile devices	2	2	4	OOS mobile devices will not operate if it is Jailbroken, based on the MDM policy.
32	Undetected technical vulnerability such as a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation.	3	3	9	OOS patches critical and high-risk vulnerabilities monthly after testing with various users across the agency.
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	3	9	The OOS has apps that are integrated with third-party cloud solutions. OOS 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	The OOS relies on the county IS&T third-party monitoring the security of our environment 24/7/365. This service keeps 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.	1	1	1	The OOS 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	1	1	The OOS secures applications to authorized personnel only.
37	Lack of training to support security awareness and strengthen compliance with security and acceptable use policies.	1	2	2	The OOS requires annual security awareness training to include acknowledgment of IT policies.
38	Lack of training materials that focus on issues such as end-point security, log-in requirements, and password administration guidelines.	3	1	3	OOS provides occasional training via the IS&T News Flash.

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	1	1	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.	2	4	8	Require all wireless networks are secured with a strong password or VPN connectivity is required to access the internal network. 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	OOS owned devices are setup to automatically connect to the OOS 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.	2	4	8	Only allow connectivity to the internal network via a VPN connection or a hardened secure software application.
43	Lack of a process to introduce application and system changes, including hardware, software, and network devices, into the IT environment.	1	3	3	OOS IT will create a change management process that includes all new hardware/software introductions.

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.
44	Lack of policies and procedures to ensure compliance with minimally acceptable system configuration requirements.	1	3	3	OSS IT will create a policy that identifies minimal acceptable system configurations allowed on the network.
45	Lack of identification of unnecessary software and services increases the potential number of discovered and undiscovered vulnerabilities in a system.	3	5	15	Third-party tools such as IDS/IPS (anti-virus) and spam filters are managed by OOS IT. Monthly maintenance is performed 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.	2	5	10	The OOS currently does not perform annual penetration testing due to lack of funding.
47	Lack of a process that defines, identifies, and classifies the vulnerabilities in a computer, network, or communications infrastructure.	2	5	10	The OOS does not have Vulnerability Management tools to identify vulnerabilities in the computing environment due to lack of funding.
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	OSS has a COOP established for the agency.

Office of the Sheriff
Clarence F. Birkhead, Sheriff

To: Darlana Moore, Mischa Preston

From: Vincent Ritter Dir. Tech/Comm

Date: December 8, 2021

Re: Technology Control Self-Assessment

This letter is to address deficiencies found in Self-Assessment. To date OOS has worked tirelessly on implementing solutions that will strengthen the network and reduce security vulnerabilities. These include hardware and software solutions, acceptable use policies and ongoing training.

In FY20-21 we began the implementation of M365 which gives us the accessibility to Multi Factor Authentication (MFA), One-Drive and Intune for Mobile Device Management (MDM). We have successfully implemented MFA but had to push back our One-Drive and Intune pieces due to a 50% reduction in staffing and a laser focus being placed on implementing Body Worn Cameras (BWC) which was one of the Sheriff's campaign initiatives and has become a very popular area of concern for our Durham County Citizens.

In speaking with the Sheriff, he has authorized the use of temporary personnel to assist in these projects and has stressed that BWCs and the MDM be completed by March 2022.