Durham County Internal Audit Department

Third Annual Information Services and Technology Control Self-Assessment

March 1, 2017

DURHAM COUNTY
DCo NC
1881

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

Audit Committee:
Harrison Shannon
Wendy Jacobs
James Hill
Manuel Rojas
Arnold Gordon

March 1, 2017

Mr. Wendell Davis,
County Manager

Dear Mr. Davis:

The Information Services and Technology (IS&T) Department has completed a high-level risk assessment at the request of Internal Audit. The risk assessment is attached.

Internal Audit has reviewed the risk assessment and believes follow-up is warranted, especially as it relates to the need for structure in the way departments obtain cloud applications. Although risks in those areas were not deemed to be high by IS&T, Internal Audit believes further audit or investigative effort should be made to assess risks related to cloud management. This issue will be included in the 2018 Annual Audit Plan.

Internal Audit believes this risk assessment provides meaningful information regarding the threats IS&T faces in securing, storing, and making data timely available. Because information and systems are never static, Internal Audit will continue to ask IS&T to conduct a Control-Self Assessment annually to keep Internal Audit and the Audit Oversight Committee apprised of its risk environment.

Sincerely,

Richard Edwards,
Internal Audit Director

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

THIRD 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 moderate

For 27 of the 33 risks Internal Audit identified and asked IS&T to rate, the assessor rated the risks as moderate. 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. However, in twenty of IS&T's responses, the assessor pointed out the need for enhanced mitigating controls departments should consider in Cloud administration. The following exhibit summarizes the frequency of ratings assigned by IS&T for the thirty-three risks Internal Audit identified.

Exhibit 1
IS&T Risk Rating for thirty-three risks

Risk Score Range	Rating	No. of risks ranked
1-8	Low	4
9-16	Moderate	27
17-25	High	2
Total Comments		33

Source: IS&T Risk Assessment

Assessor responses require additional review

In fiscal year 2018, Internal Audit will review departmental uses of Cloud applications to provide management with assurance that the risks are being managed to an acceptable level. In providing that assurance, Internal Audit will determine the level of business risk present and what can be done to lessen the risk, especially as it relates to Cloud applications. During discussions about Cloud applications with IS&T representatives, we were told that departments that need specific or unique business applications may acquire them outside of the IS&T's guidance. We were also told that IS&T is not sure of the number of Cloud applications being used in the County, but IS&T is aware of approximately eighty-one applications. According to the risk assessor's comments, departments may not have tools to assure that their data is secure and that it will be accessible when needed.

In the comment section of the following risk assessment, the risk assessor provided statements and some of them are mentioned below.

- In five (5) instances, the risk assessor said "[c]urrently, there is no formal guidance or standards for DCo Departments to utilize when negotiating a contract for cloud services."

- In four (4) instances, the risk assessor replied "[a] County department that utilizes a cloud service must understand their specific responsibilities and implement appropriate processes to address them."

- In four (4) instances, the risk assessor stated that departments "…should consider developing a business continuity plan (i.e. paper-based procedures) in order to maintain operations during system outages."

- In three (3) instances, the risk assessor reported that "DCo should consider developing a cloud contract terms and conditions template to ensure critical contractual issues such as security safeguard expectations are clearly defined in the contract."

- In one (1) instance, the risk assessor stated "…currently it is up to each department that used the cloud to develop, communicate and enforce related policies and procedures to cloud users."

- In one (1) instance, the risk assessor replied "DCo should consider developing a guidance document for all departments to use [the cloud]."

Based upon these comments, Internal Audit will propose to conduct an audit of cloud user controls within the County. The proposal will be included in the 2018 Annual Plan.

Third 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.	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	Malware attacks through e-mails	2	5	10	DCo receives hundreds of emails daily that contain malware. IS&T uses a "defense in layers" architecture to scan and review each email thoroughly, using multiple technologies, to remove any malicious software found from the message before it is released to the recipient's Inbox. IS&T continually evaluates the growing variety of threats and recommends changes/improvements as required. Additionally IS&T utilizes a security awareness process to remind employees not click on links in suspicious emails. While no process is 100% foolproof, this layered defense strategy provides reasonable safeguards to mitigate the risk.
2	Malware attacks through the web	2	5	10	The IS&T firewalls use anti-malware software to scan all web activity. As a second line of defense, anti-malware software is installed on each PC and server that malware would try to infect. This layered defense strategy provides reasonable safeguards to mitigate the risk.
3	Malware attacks through file shares	2	5	10	In addition to the anti-malware scanning performed on all incoming email and Internet downloads, IS&T has installed anti-malware scanning software on all file servers and PCs where file shares and folders reside. This layered defense strategy provide reasonable safeguards to mitigate the risk.
4	Malware attacks through mobile devices	2	3	6	While currently not a significant threat, mobile malware continues to grow in both complexity and in the number of emerging viruses. Mobile malware is a growing threat that requires monitoring.

	Threats	**Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.**	**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.**
5	Deceptive practices that introduce malware into computer systems (i.e., Phishing and Rogue Security Software)	2	5	10	The layered anti-malware defenses described in 1, 2, and 3 above provide reasonable safeguards to mitigate the risk.
6	Malicious Spyware	2	5	10	Spyware is just a sub-category of malware. The layered anti-malware defenses described above provide reasonable safeguards to mitigate the risk.
7	Password Cracking	1	5	5	DCo's network password standards conform to industry best practices - a minimum of 8 characters and must contain at least 3 elements of complexity (Upper case, lower case, numbers, and special characters). In addition, a user's account is locked after 5 invalid attempts and the password must be changed every 90 days. If an attacker has enough time, any password can be cracked; however, IS&T has implemented reasonable safeguards to mitigate the risk.
8	Malicious Insiders (comprise/ consultants) who intentionally introduce malware into computer systems	1	5	5	The layered anti-malware defenses described in 1, 2, and 3 above provide reasonable safeguards to mitigate the risk.

	Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	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.
9	Inadequate existing applications that fail to protect sensitive data	2	5	10	The current DCo portfolio of applications do have varying levels of built-in security; however, when combined with the IS&T layered security defenses (i.e. firewalls, anti-malware software, etc.) reasonable safeguards are in place to mitigate the risk.
10	Insufficient training and education about security risks for comprise/ authorized workers	3	5	15	IS&T is currently working to improve its security awareness program to provide employees with specific guidance for making better security decisions while performing the daily jobs.
11	Lack of policies or unclear policies regarding users' access to Cloud data	3	5	15	Currently there are no specific policies in place to provide guidance on Cloud access and data usage.
12	Cloud security system failures	2	5	10	Cloud systems are generally designed to be highly reliable and redundant; however, system failures are still possible. DCo should consider developing a Cloud contract terms and conditions template to ensure critical contractual issues, such as service level contracts and penalties for non-compliance, are defined in the contract. Additionally, if the DCo Department is highly dependent on the cloud service, they should consider developing a business continuity plan (i.e. paper-based procedures) in order to maintain operations during system outages.

	Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	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	Cloud storage and database server failures	2	5	10	Cloud systems are generally designed to be highly reliable and redundant; however, system failures are still possible. DCo should consider developing a Cloud contract terms and conditions template to ensure critical contractual issues, such as service level contracts and penalties for non-compliance, are defined in the contract. Additionally, if the DCo Department is highly dependent on the cloud service, they should consider developing a business continuity plan (i.e. paper-based procedures) in order to maintain operations during system outages.
14	Inadequate security measures implemented by the County to prevent Cloud hacking/ unauthorized intrusions	3	5	15	As noted in No. 11 above, no policies exist to help guide DCo departments. Cloud security is a shared responsibility between the vendor and customer. Each County Department that utilizes a cloud service must understand their specific responsibilities and implement appropriate processes to address them.
15	Inadequate security measures implemented by Cloud Vendor/ Service Provider to prevent Cloud hacking/ unauthorized intrusions	2	5	10	In general, cloud vendors have robust security safeguards in place designed specifically for their application. However, ultimately Cloud security is a shared responsibility between the vendor and customer. The County department that utilizes a cloud service must understand their specific responsibilities and implement appropriate processes to address them. Additionally DCo should properly vet a vendor's security safeguards prior to entering into a contract. DCo should consider developing a Cloud contract terms and conditions template to ensure critical contractual issues, such as security safeguard expectations, are clearly defined in the contract.

	Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	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.
16	Unclear location of Cloud data	3	2	6	Cloud systems by design are very fluid as to the location of data. Data can be stored in multiple locations within the U.S. or overseas. DCo should consider developing a Cloud contract terms and conditions template to ensure critical contractual issues, such as specifying the desired location of DCo data, are defined in the contract.
17	Cloud data loss or leakage	2	5	10	Cloud systems are generally designed to be highly reliable and secure; however, data loss/leakage is still possible. DCo should consider developing a Cloud contract terms and conditions template to ensure critical contractual issues, such as security safeguards, have been vetted prior to signing a contract as well as DCo expectations for security are fully defined in the contract.
18	Cloud data becomes corrupted	2	5	10	Cloud systems are generally designed to be highly reliable and redundant; however, data corruption is still possible. DCo should consider developing a Cloud contract terms and conditions template to ensure critical issues such as, data redundancy and data restoration, have been reviewed and defined in the contract. Additionally, if the DCo Department is highly dependent on the cloud service, they should consider developing a business continuity plan (i.e. paper-based procedures) in order to maintain operations during system outages.

	Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	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.
19	Inadequate Cloud data backup and disaster recovery process	2	5	10	Cloud systems are generally designed to be highly reliable and redundant; however, disaster recovery events are still possible. DCo should consider developing a Cloud contract terms and conditions template to ensure critical contractual issues, such backups and disaster recovery requirements, are defined in the contract. Additionally, if the DCo Department is highly dependent on the cloud service, they should consider developing a business continuity plan (i.e. paper-based procedures) in order to maintain operations during system outages.
20	Failure to communicate Cloud related policies and procedures to Cloud users	3	5	15	Currently there are no centralized policies to provide guidance to DCo employees on Cloud access and data usage. Currently it is up to each DCo Department that is using a cloud service to develop, communicate, and enforce related policies and procedures to cloud users. DCo should consider developing a guidance document for all departments to use.
21	Cloud users delete Cloud data	3	5	15	The deletion of cloud data by a user, either intentionally or accidently, is very possible. However, this is not unique to cloud systems. Systems hosted within DCo have the same risk. Depending on how quickly the data loss is detected and how far back the data backups go will determine whether the data can be recovered. DCo should consider developing a Cloud contract terms and conditions template to ensure critical contractual issues, such as data backup expectations, are included in the contract.

	Threats	**Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.**	**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.**
22	Lack of security measures to protect sensitive/ private data in the Cloud	2	5	10	In general, cloud vendors have robust security safeguards in place designed specifically for their application. However, ultimately Cloud security is a shared responsibility between the vendor and customer. The County department that utilizes a cloud service must understand their specific responsibilities and implement appropriate processes to address them. Additionally DCo should properly vet a vendor's security safeguards prior to entering into a contract. DCo should consider developing a Cloud contract terms and conditions template to ensure critical contractual issues, such as security safeguard expectations, are clearly defined in the contract.
23	Insufficient means to identify Cloud data breaches	2	5	10	In general, cloud vendors have robust security safeguards in place designed specifically for their applications. However, DCo should clearly communication expectations on communicating data breach in the contract. Currently there is no formal guidance or standards for DCo Departments to utilize when negotiating a contract for cloud services. DCo should consider developing a Cloud contract terms and conditions template to ensure critical issues as well as legal remedies are clearly defined in the contract.

	Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	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	Cloud Vendor/ Service Provider has rights to use certain data stored in the County Cloud for its own purposes	4	5	20	Many vendors can and will use customer data, usually identified, for their own research purposes and/or resale. Currently there is no formal guidance or standards for DCo Departments to utilize when negotiating a contract for cloud services pertaining to data ownership. DCo should consider developing a Cloud contract terms and conditions template to ensure critical issues as well as legal remedies are clearly defined in the contract.
25	Cloud Vendor/ Service Provider's other customers gain access to County data stored in the Cloud	2	5	10	In general, cloud vendors have robust security safeguards in place designed specifically for their application. However, ultimately Cloud security is a shared responsibility between the vendor and customer. The County department that utilizes a cloud service must understand their specific responsibilities and implement appropriate processes to address them. Additionally DCo should properly vet a vendor's security safeguards prior to entering into a contract. DCo should consider developing a Cloud contract terms and conditions template to ensure critical contractual issues, such as security safeguard expectations, are clearly defined in the contract.
26	Cloud service contract fails to specify Durham County's ownership of Cloud data	2	5	10	See 24 above. Currently there is no formal guidance or standards for DCo Departments to utilize when negotiating a contract for cloud services. DCo should consider developing a Cloud contract terms and conditions template to ensure critical issues as well as legal remedies are clearly defined in the contract.

	Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	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	Cloud service contract fails to identify who is responsible for data breach notifications	3	5	15	Also, see 23 above. Currently there is no formal guidance or standards for DCo Departments to utilize when negotiating a contract for cloud services. DCo should consider developing a Cloud contract terms and conditions template to ensure critical issues as well as legal remedies are clearly defined in the contract.
28	Cloud service contract fails to specify liability upon data breaches and data loss	3	5	15	Currently there is no formal guidance or standards for DCo Departments to utilize when negotiating a contract for cloud services. DCo should consider developing a Cloud contract terms and conditions template to ensure critical issues as well as legal remedies are clearly defined in the contract.
29	Lack of transparency in Cloud Vender/ Service Provider operations	3	3	9	Depending on cloud services being provided, the impact from the lack of transparency to DCo could range from none to significant. By design, Cloud service operations are managed by the vendor; however, the lack of openness regarding major issues such as cybersecurity issues, inadequate computing infrastructure or resources, financial or legal woes, etc. could result in unplanned/anticipated service disruptions or legal issues. Specific requirements regarding transparency and communication must be defined in the contract in order to protect DCo.
30	Lack of Vendor/ Service Provider accountability for failure to provide services	5	5	25	DCo should consider developing a Cloud contract terms and conditions template to ensure critical issues as well as legal remedies are clearly defined in the contract.

	Threats	Probability (P) The likelihood that an adverse event will occur. Rate 1 to 5 with 1 being the least likelihood.	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.
31	Cloud Vendor/ Service Provider goes out of business	2	5	10	DCo should consider developing a Cloud contract terms and conditions template to ensure critical issues as well as legal remedies are clearly defined in the contract.
32	Inadequate procedures to transfer Cloud data to an alternate Vendor/ Service Provider when contractual relationship with current Vendor ends	3	5	15	DCo should consider developing a Cloud contract terms and conditions template to ensure critical issues as well as legal remedies are clearly defined in the contract.
33	Legal/financial consequences occur due to Durham County terminating Cloud service contract with Vendor/ Service Provider	3	5	15	DCo should consider developing a Cloud contract terms and conditions template to ensure critical issues as well as legal remedies are clearly defined in the contract.