Mecklenburg County
Department of Internal Audit

Public Information Department
Social Media Program
Report 1763

June 14, 2018

Internal Audit's Mission	To support key stakeholders in cultivating an environment of accountability, transparency, and good governance.
Internal Audit Contacts	Joanne Prakapas, CPA/CFF, CIA, CRMA, CFE, Audit Director (980) 314-2889 or joanne.prakapas@mecklenburgcountync.gov Felicia Stokes, CIA, CISA, CRMA, Audit Manager (980) 314-2893 or felicia.stokes@mecklenburgcountync.gov
Staff Acknowledgements	Frank Crutchfield, CIA, CRMA, CISA, Auditor-in-Charge
Obtaining Copies of Internal Audit Reports	This report can be found in electronic format at https://www.mecknc.gov/audit/reports/pages/default.aspx

MECKLENBURG COUNTY
Department of Internal Audit

To: Danny Diehl, Director, Public Information Department

From: Joanne Prakapas, Director, Department of Internal Audit

Date: June 14, 2018

Subject: Social Media Program Report 1763

The Department of Internal Audit has completed its audit of the Public Information Department's social media program to determine whether internal controls effectively manage key business risks inherent to this activity. Internal Audit interviewed key personnel; reviewed and evaluated policies, procedures, and other documents; observed operations; and tested various activities from September 30, 2014 through September 30, 2017.

This audit was conducted in conformance with The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

OVERALL EVALUATION

Overall, the management of key risks inherent to the social media program were managed to an acceptable level; however, opportunities exist to improve the design and operation of some control activities.

RISK OBSERVATION SUMMARY

The table below summarizes the risk observations identified during the audit, grouped by the associated risk factor, and defined in Appendix A. The criticality or significance of each risk factor, as well as Internal Audit's assessment of the design and operation of key controls to effectively mitigate the risks, are indicated by the color codes described in Appendix B.

RISK OBSERVATION SUMMARY			
Risk Factors and Observations	**Criticality**	**Design**	**Operation**
1. Policies and Procedures Risk	🔴	🟡	🟡
1.1 Formal Documentation 1.2 Annual Review			
2. Human Resource Risk	🟡	🟡	🟡
2.1 Staff Training			
3. System Access Risk	🟡	🟡	🟡
3.1 Access Management 3.2 Password Management			
4. Compliance Risk	🟡	🟢	🟢
No risk observation noted			
5. Authorization Risk	🟡	🟢	🟢
No risk observations noted			
6. Reputational Risk	🟡	🟢	🟢
No risk observations noted			
7. Segregation of Duties Risk	🟡	🟢	🟢
No risk observations noted			

The risk observations and management's risk mitigation strategies defined in Appendix C are discussed in detail in the attached document. Internal Audit will conduct a follow-up review to verify management's action plans have been implemented and are working as expected.

We appreciate the cooperation you and your staff provided during this audit. Please feel free to contact me at 980-314-2889 if you have any questions or concerns.

c: County Manager
Assistant County Manager/Chief of Staff
Assistant County Managers
Deputy County Attorney
Senior County Attorney
Board of County Commissioners
Audit Review Committee

BACKGROUND

The mission of the Public Information Department social media program is to tell Mecklenburg County's story through websites and applications that enable users to create and share information.

The social media program's objectives are to:

- Increase resident involvement and engagement on all social media platforms
- Coordinate the social media presence across all departments to ensure consistency, accuracy, compliance, and best practice
- Increase employee awareness of and engagement with the County's social media presence

ORGANIZATION

The Public Information Department (PI) Director oversees the social media program. The social media coordinator (coordinator) and social media specialist (specialist) positions were both created in 2016 to assist in managing daily program activities across the County's seven active social media platforms, i.e., Twitter, Facebook, Flickr, Nextdoor, LinkedIn, Instagram, and YouTube. These platforms serve as a tool to disseminate information to County residents and allow them to submit real time general inquiries to a specific department; voice concerns over a topic; and provide feedback on social media content posted by the County. Additionally, the County has 21[1] departmental administrators that aid in posting content, monitoring accounts, and responding to public comments.

The coordinator evaluates all new social media account requests submitted online by department representatives, and determines whether the accounts have a business purpose before approving the requests. When an account is not approved, the coordinator may accommodate the request by posting content to an existing County social media channel.

The coordinator ensures passwords for all social media accounts managed by the County adhere to policy by changing passwords on a quarterly basis and when staff is terminated or reassigned**.** Password change notifications are primarily sent electronically to account administrators but may sometimes be communicated during department meetings.

In January 2017, the coordinator implemented formal training for some social media staff, replacing the ad hoc training given only to departments with substantial social media use.

Social Media Content

The coordinator and specialist can post content directly to a social media account or use their third-party social media management software, which centralizes social media account activity. Department administrators, however, can only post content directly to their account(s). Content may be posted immediately or scheduled for a future date.

[1] As of May 10, 2018

Monitoring

The social media program policy requires department administrators monitor public comments on a daily basis. When an inquiry requires a response, one should be posted within 24 hours on a work day or 48 hours on a holiday or weekend.

The coordinator and specialist periodically review social media activity using their media management software to ensure compliance with policy and procedures. The coordinator creates a task in the software to document their review.

Archiving

All information and feedback shared on County social media platforms are public records. To retain these records, the County uses a social media archiving tool, which interfaces with the County's social media platforms, capturing all activity, including hidden and deleted comments.

COUNTY MANAGER’S OVERALL RESPONSE

The County Manager concurs with all risk mitigation strategies and timeframes for implementation.

RISK OBSERVATIONS AND MITIGATION STRATEGIES

Risk Factor	Criticality	Design	Operation
1. Policies and Procedures Risk	🔴	🟡	🟡

Risk Observations

1.1 Formal Documentation—Some formal, documented policies and procedures for the social media program administration did not always reflect current and/or best practices. Yet, policies and procedures are important control activities to help ensure management’s directives are carried out while mitigating risks that may prevent the organization from achieving its objectives.

1.2 Annual Review—The Department’s social media program policy indicates it will be annually reviewed. While there was evidence the policy was reviewed in May 2017, there was no evidence the reviews took place in 2015 and 2016.

Recommendations

1.1 Internal Audit recommends management develop and implement formal, documented policies and procedures for all social media program activities and train staff accordingly. The policies and procedures should include, at a minimum:

- Policy and procedure reviews and updates
- Staff training and oversight
- Staff roles and responsibilities

1.2 Internal Audit recommends management annually review the social media policy and procedures and document their review.

Management’s Responses

1.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** August 2018

Action Plan: The social media policy is currently under annual review by the social media coordinator and will incorporate a procedure for review of the policy, more details on staff training, roles, and responsibilities.

1.2 **Risk Mitigation Strategy:** Reduce **Implementation Date:** August 2018

Action Plan: The social media policy is currently under annual review by the social media coordinator. All annual reviews will be documented moving forward.

Risk Factor	Criticality	Design	Operation
2. Human Resource Risk	🟡	🟡	🟡

Risk Observation

2.1 Staff Training—Social media program management did not ensure all administrators completed routine training, nor did management consistently document evidence of the training. Without proper training, management cannot ensure social media administrators, who are responsible for posting and reviewing social media content, receive the information needed to effectively manage their social media activities.

Recommendation

2.1 Internal Audit recommends management ensure social media staff receives routine training and appropriately documents and maintains evidence that training was received.

Management's Response

2.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** August 2018

Action Plan: In December of 2017 we conducted a review of administrators who had access to social media accounts but were not actively managing those accounts or participating in training. We eliminated some and re-established expectations with others.

To further reduce risk moving forward, we will establish expectations for training in the policy and with administrators and their managers. We will continue to monitor administrator performance on an ongoing basis.

Risk Factor	Criticality	Design	Operation
3. System Access Risk	🟡	🟡	🟡

Risk Observations

3.1 Access Management—While the coordinator or specialist changed passwords on a quarterly basis for social media accounts managed by the County, there is no process in place to identify and ensure account access was timely deactivated for terminated staff and prior account administrators. Without appropriate system access management, unauthorized persons could publish inappropriate information on behalf of the County.

3.2 Password Management—Social media program management did not always maintain documentation of required quarterly password changes for social media accounts. Without appropriately documenting password changes, management has limited ability to ensure the department is compliant with County password policy.

Recommendations

3.1 Internal Audit recommends management establish and implement a process to timely identify terminated staff and inactive administrators, promptly deactivate their social media account access, and maintain documentation of the deactivations.

3.2 Internal Audit recommends management ensures staff documents and maintains evidence that quarterly social media password changes were completed.

Management's Responses

3.1 **Risk Mitigation Strategy:** Transfer **Implementation Date:** August 2018

Action Plan: We will develop a process to notify managers once per year who on their staff is a social media administrator, the risk involved with a terminated employee having access to social media accounts and ask them to notify us when a social media administrator has been terminated so we can deactivate their account access and document it.

3.2 **Risk Mitigation Strategy:** Reduce **Implementation Date:** August 2018

Action Plan: We will begin maintaining this quarterly documentation with our next quarterly password change in August 2018.

APPENDIX A—Risk Factor Definitions

Risk Factor	Definition
Authorization Risk	Failure to clearly articulate and communicate those with the authority to commit the organization may result in internal and external misunderstandings.
Compliance Risk	Failure to comply with established policies, procedures, and/or statutory requirements may result in unacceptable performance that impacts financial, operational, or customer objectives.
Human Resource Risk	Failure to attract, train, develop, deploy, and/or empower competent personnel may inhibit the organization's ability to execute, manage, and monitor key business activities.
Policies and Procedures Risk	Failure to have formal, documented, clearly stated, and updated policies and procedures may result in poorly executed processes and/or increased operating costs.
Reputational Risk	Failure to maintain an organization’s reputation may result in lost revenue; increased operating, capital, regulatory, or legal expenses; and destruction of stakeholder value and/or public trust.
Segregation of Duties Risk	Failure to adequately segregate duties may allow an employee or group of employees to perpetrate and conceal errors or irregularities without timely detection.
System Access Risk	Failure to appropriately restrict access to data or programs may result in unauthorized changes, inappropriate access to restricted or confidential information, or inefficiencies where access is too restrictive.

APPENDIX B—Color Code Definitions

The criticality of a risk factor represents the level of potential exposure to the organization and/or to the achievement of process-level objectives before consideration of any controls in place (inherent risk).

Criticality	Significance and Priority of Action
🔴	The inherent risk poses or could pose a significant level of exposure to the organization and/or to the achievement of process level objectives. Therefore, management should take immediate action to address risk observations related to this risk factor.
🟡	The inherent risk poses or could pose a moderate level of exposure to the organization and/or to the achievement of process level objectives. Therefore, management should take prompt action to address risk observations related to this risk factor.
🟢	The inherent risk poses or could pose a minimal level of exposure to the organization and/or to the achievement of process level objectives. Risk observations related to this risk factor, however, may provide opportunities to further reduce the risk to a more desirable level.

The assessment of the design and operation of key controls indicates Internal Audit's judgment of the process and system design to mitigate risks to an acceptable level.

Assessment	Design of Key Controls	Operation of Key Controls
🔴	The process and system design does not appear to be adequate to manage the risk to an acceptable level.	The operation of the process' risk management capabilities is not consistently effective to manage the risk to an acceptable level.
🟡	The process and system design appear to be adequate to manage the risk to an acceptable level. Failure to consistently perform key risk management activities may, however, result in some exposure even if other tasks are completed as designed.	The operation of the process' risk management capabilities is only partially sufficient to manage the risk to an acceptable level.
🟢	The process and system design appear to be adequate to manage the risk to an acceptable level.	The operation of the process' risk management capabilities appears to be sufficient to manage the risk to an acceptable level.

APPENDIX C—Risk Mitigation Strategy Definitions

Risk Mitigation Strategy	Definition
Reduce	Risk response where actions are taken to reduce a risk or its consequences.
Accept	Risk response where no action is taken to affect the risk.
Transfer	Risk response where a portion of the risk is transferred to other parties.
Avoid	Risk response to eliminate the risk by avoiding or withdrawing from the activity giving rise to the risk.