Mecklenburg County
Department of Internal Audit

Information Technology Services
Incident Response Management
Report 1952

October 12, 2020

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

Christopher Waddell, CIA, CRMA, Audit Manager
(980) 314-2889 or christopher.waddell@mecklenburgcountync.gov

Staff Acknowledgements

Eric Davis, CIA, CISA, CRMA, 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: Keith Gregg, Chief Information Officer
Information Technology Services

From: Joanne Prakapas, Director
Department of Internal Audit

Date: October 12, 2020

Subject: Incident Response Management Report 1952

The Department of Internal Audit has completed its audit of the incident response management process to determine whether controls effectively manage key business risks inherent to this activity. Internal Audit interviewed key personnel; observed operations; reviewed and evaluated policies and procedures; and tested major incident response activities from July 1, 2015 through May 31, 2019.

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, key risks inherent to the incident response management process 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			
2. Incident Management Risk	🔴	🟡	🟡
2.1 Incident Response Resources 2.2 Response Resolution Times			
3. Human Resources Risk	🟡	🟡	🟡
3.1 Staff Training			
4. Documentation Risk	🔴	🟡	🟡
4.1 Incident Documentation			
5. Segregation of Duties Risk	🔴	🟢	🟢
No risk observations noted			
6. Performance Measurement Risk	🟡	🟢	🟢
No risk observations noted			
7. Compliance 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 Managers
County Attorney
Deputy County Attorney
Board of County Commissioners
Audit Review Committee

BACKGROUND

Mecklenburg County's Information Technology Services (the Department) provides information technology (IT) services that support all County business operations and service delivery to the public. A critical aspect of this service includes maintaining the integrity, availability, and reliability of the IT environment, of which incident management is an essential element.

Incident Management

Incident management is an area of IT service management (ITSM) that includes the process or set of activities used to identify, understand, and resolve IT-related issues. The goal of incident management is to restore normal service operation as quickly as possible with minimum disruption to the organization.

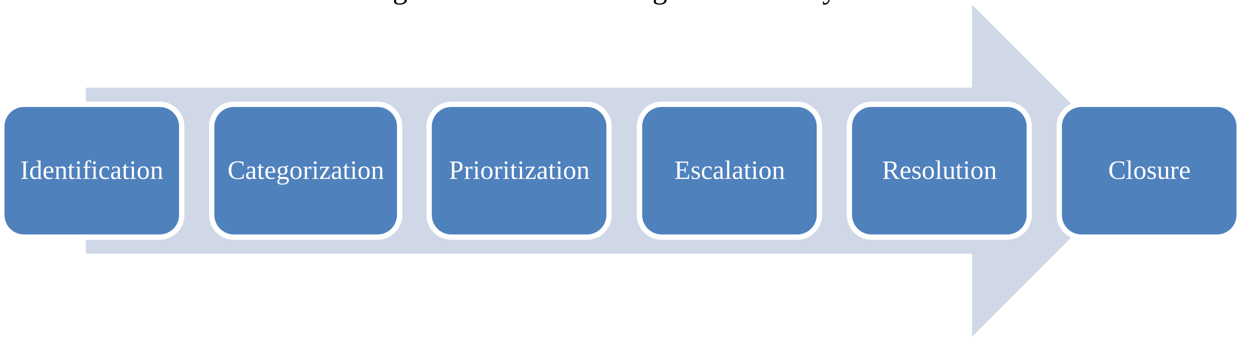
Incidents

An event is any observable occurrence in the IT infrastructure such as receiving an email or a system reboot, which may be a benign event or could provide an indication that an incident is occurring. An IT incident, on the other hand, is an unexpected event that disrupts the normal operation of an IT service, e.g., a distributed denial of service (DDos) attack or an IT server room flooding. A security event is an event that could affect information security specifically. A security incident has a similar relationship to a security event in that it specifically affects information security, normally by violating a security policy. Events and incidents are not mutually exclusive; and while all incidents are events, not all events are incidents.

Incident Management Lifecycle

In ITSM, most incidents are managed in a lifecycle approach that involves identification, categorization, prioritization, escalation, resolution, and closure steps. Specific workflows and processes may differ depending on the way an IT organization works and the incident they are addressing. Figure 1 below depicts a basic incident management lifecycle process.

Figure 1: Incident Management Life Cycle



- *Identification, categorization, and prioritization* activities determine the right course of action, including an assessment of impact and urgency, the extent of communication needed, who should handle the resolution, and the speed of the response. For example, a major incident would be one that has a significant impact and urgency and demands an efficient response.

- *Escalation* activities occur throughout the process and typically require higher-level specialist teams with better capability to address an incident, as well as higher level management that can make the necessary decisions regarding communications, emergency changes, and/or required resources.

- *Resolution* activities seek to contain, investigate, and resolve incidents. These activities can involve several service teams within IT to mitigate incidents, as well as repair and recover, if necessary, affected systems or data.

- *Closure* activities assess how effectively an incident response was executed during an incident, such as identifying lessons learned and making security and process improvement changes.

Major Incident Activity

From FY 2016 to FY 2019, the Department handled 369 major incidents, which included four security incidents. The following table summarizes the number of incidents each fiscal year.

Information Technology Services
Incidents by Year

Incident Type	FY 2016	FY 2017	FY 2018	FY 2019
All Incidents	32,278	29,447	26,656	27,888
Major Incidents	127	94	67	81
Major Security Incidents	1	1	2	0

Source: Auditor analysis of department data, unaudited

COUNTY MANAGER'S OVERALL RESPONSE

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

RISK OBSERVATIONS AND MITIGATION STRATEGIES

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

Risk Observation

1.1 Formal Documentation—While the Department had formal, documented procedures for aspects of its incident management process, the procedures did not reflect current and/or best practices. For example, the Department did not have procedures specific to handling security incidents. Nor did it have an incident management policy and plan governing incident management. Yet, policies and procedures are important control activities to help management ensure its directives are carried out while mitigating risks that may prevent the organization from achieving its objectives.

Recommendation

1.1 Internal Audit recommends management formally develop and implement an incident management policy and plan and update its standard operating procedures, consistent with applicable County requirements and aligned to industry-recognized best practices. Procedures should include incident management lifecycle activities specific to security incidents. All staff involved in incident management activities should be trained accordingly.

Management's Response

1.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** December 2020

Action Plan: The Department will develop department procedures and train staff accordingly. The procedures will be reviewed on an annual basis to ensure they are up-to-date and reflect current and best practices.

Risk Factor	Criticality	Design	Operation
2. Incident Management Risk	🔴	🟡	🟡

Risk Observations

2.1 Incident Response Resources—A "jump kit" with resources such as laptops with appropriate software, backup devices, blank media, networking equipment, network diagrams, current baselines and access to clean images was not readily available to assist with incident handling. Best practice recommends incident response teams keep a jump kit of important tools on hand so in the event of a security incident, they can initiate a "grab-and-go" to facilitate a timely response.

2.2 Response Resolution Times—The incident response process defines required timeframes for incidents to be resolved to ensure timely response to disruptions in the IT environment. Resolution timeframes are established based on an incident's assessed impact and urgency. However, 27 of 39 or 69% of major incidents sampled were not resolved within targeted timeframes. Failure to respond and resolve incidents timely may result in a greater loss of or longer disruption to business operations or services, adversely impacting information security, information systems, employees, customers, or other critical business functions.

Recommendations

2.1 Internal Audit recommends management create and maintain an appropriate number of jump kits based on the organization's size and potential need.

2.2 Internal Audit recommends management evaluate whether current response timeliness metrics are appropriate and identify any potential process improvement opportunities. The evaluation and results should be formally documented.

Management's Responses

2.1 **Risk Mitigation Strategy:** Accept **Implementation Date:** N/A

Action Plan: Covering all variable possibilities relating to incidents with "jump kits" would be financially impractical for the county. IT employs various methods to minimize catastrophic losses while maximizing the ability to resolve problems and major incidents (i.e. some equipment is maintained for mobile devices that can quickly be imaged and distributed, Vendor agreements that include response times, redundancy and resiliency built into infrastructure environments…etc.).

ITS has implemented several new projects over the past 3 years to help minimize the downtime or catastrophic losses to the County. ITS established a secondary data center in Atlanta, Georgia with up-to-date technology and verified connectivity to both the internet and Microsoft Azure, the cloud service provider Mecklenburg County uses most frequently. This secondary data center can be spun up quickly should the County lose all internet capacity in Charlotte, NC at the primary Flexential Data Center. ITS Network Services also just completed the multimillion-dollar project to replace core networking equipment and data closet switch replacement. The equipment chosen included specifications to ensure maximum uptime for a cost that the County found reasonable and acceptable. The equipment was outfitted with dual power supplies and dual supervisory cards to minimize outages due to equipment failure. The County also carries extended warranty on this equipment and allows for replacement equipment to be onsite within one business day. ITS Engineering and Storage recently replaced the backup equipment with new equipment that allows for backups to occur throughout the day (based on the application) and offsite backups are stored in a secure location in the cloud. Backup of mission critical applications can occur within hours instead of days or weeks. Additionally, we utilize VM Ware's latest technologies that allow us to spin up new virtual servers within minutes should we have a "server failure" and backups would be pulled from the backup appliance to restore the application and or server. In addition to utilizing on premise equipment where we can spin up new virtual servers, we have the ability to use virtual equipment in the Microsoft Azure Cloud if needed.

New development performed by our ITS Application Development Team looks first towards programming and hosting in the Cloud (Microsoft Azure and Dynamics) so we can utilize the built in DR opportunities provided to Microsoft's clients.

ITS does keep a small inventory of laptops and desktops on hand to provide hot swap equipment to end users should their existing equipment fail. These laptops can be used in the event of a disaster or catastrophic event. The use of soft phones has also increased since the onset of COVID 19 and this allows Mecklenburg County to "dial from their computer" rather than having to utilize a physical phone. Our telecom and mobile teams also have loaner cell phone equipment handy for use by end users if their equipment is lost, stollen or broken, but this equipment could also be used in the event of a disaster.

While we do not recommend having cold equipment on standby because this equipment is very costly, we feel that we have made appropriate replacements of outdated equipment over the past several years with equipment that is designed to run in a degraded state until it can be formally replaced, thus minimizing loss or downtime.

2.2 **Risk Mitigation Strategy:** Reduce **Implementation Date:** December 2020

Action Plan: The Incident Management Team has met and determined that the timeliness metric will be addressed with the implementation of the new Everbridge IT Alerting Tool. This is currently being implemented and will be completed by FY21 Q2 (end of the calendar year). Cherwell will continue to track all tickets and incidents and Everbridge will help with recording the happenings of the event. It should be noted in the current system, Problem Records involving Major Incidents are often left open for several weeks while root cause analysis is completed. The actual incident however is closed upon the fix being applied. The Department can provide additional information to Internal Audit reflecting when the incident was resolved, but the record stayed open for root cause analysis. Lastly, we are adding a start and end date and a time field on the Problem Record to help accurately reflect how long it takes to resolve Major Incidents.

Risk Factor	Criticality	Design	Operation
3. Human Resources Risk	🟡	🟡	🟡

Risk Observation

3.1 Staff Training—Although the Department had a multi-faceted approach to address staff training, which included a mix of internal and external training, it did not have a comprehensive training program for staff responsible for incident management. Yet, formal training in incident management helps ensure staff have the necessary knowledge and skills when responding to incidents.

Recommendation

3.1 Internal Audit recommends management provide formal training on incident management for all staff that may be involved in the process. Training content should be periodically reviewed and updated as necessary.

Management's Response

3.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** December 2020

Action Plan: The Department recognizes that the staff specifically assigned to handle incident management requires ongoing training to maintain their skills. For each person identified as having the Incident Management Role as part of their job description, IT will require at least one of their individual development goals associated with their Annual Review Document process be specifically targeted towards incident management. The supervisor of that employee will work with staff to determine what level of training and the IT Incident Management topic should be covered in that fiscal year as they best understand the needs of the unit. Additionally, the Department will include training for all IT Staff during their regularly scheduled All IT Meetings and will occur at least annually to ensure staff are aware of the expectation of participation in incidents. This training will include how ITS handles IT Incident Management for any level of incident. Historically, ITS has completed at least one IT Tabletop Exercise and included in this exercise are the steps ITS would take to respond to the issue.

Risk Factor	Criticality	Design	Operation
4. Documentation Risk	🔴	🟡	🟡

Risk Observation

4.1 Incident Documentation—Security incidents deemed low in impact and urgency were not consistently documented and subjected to formal incident management procedures. Without proper documentation, security incidents may not be properly tracked and monitored to ensure timely resolution and restoration to normal operations. In addition, remediation strategies for future events or lessons learned may be lost instead of being utilized to improve the overall effectiveness of the incident management process.

Recommendation

4.1 Internal Audit recommends management document all security incidents and related information throughout the incident's lifecycle. For example, how the incident was identified, the scope of the incident, and how the incident was contained and eradicated.

Management's Response

4.1 **Risk Mitigation Strategy:** Reduce **Implementation Date:** December 2020

Action Plan: Management will ensure that all incidents regardless of impact or urgency are documented in the ticketing system. This topic has been discussed numerous times at staff meetings and will continue to be emphasized by the Security Operation Center Supervisor. Lastly, Incident Reporting is outlined in the Incident Response Plan and staff is expected to follow all agency policies, procedures and standard operation procedure manuals.

APPENDIX A—Risk Factor Definitions

Risk Factor	Definition
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.
Documentation Risk	Failure to adequately collect, file, and retain key documentation may result in lack of accountability and/or evidence to support transactions and events.
Human Resources 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.
Incident Management Risk	Failure to properly manage and respond to information technology (IT) incidents, such as a system breach or outage, could result in the organization’s inability to operate critical IT systems and applications.
Performance Measurement Risk	Failure to have defined metrics and the ability to gather relevant information for measurement purpose may impair management's ability to monitor individual, team, and/or overall business performance.
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.
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.

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 do 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.