Mecklenburg County
Department of Internal Audit

Change Management Audit
Report 1552

February 26, 2016

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, CFE, CRMA, Audit Director (980) 314-2889 or joanne.prakapas@mecklenburgcountync.gov Christopher Waddell, CIA, CRMA, Audit Manager (980) 314-2888 or christopher.waddell@mecklenburgcountync.gov
Staff Acknowledgements	Richard Kring, CISA, Auditor-In-Charge Deborah Caldwell, CIA, CISA, Information Technology Auditor
Obtaining Copies of Internal Audit Reports	This report can be found in electronic format at http://charmeck.org/mecklenburg/county/audit/reports/pages/default.aspx

MECKLENBURG COUNTY
Department of Internal Audit

To: Keith Gregg, Chief Information Officer, Information Technology

From: Joanne Prakapas, Director, Department of Internal Audit

Date: February 26, 2016

Subject: Change Management Audit Report 1552

The Department of Internal Audit has completed its audit of the Information Technology Services' change management process and related practices to determine whether internal controls effectively manage key risks inherent to change management. Internal Audit staff interviewed key personnel, observed operations, reviewed and evaluated policies and procedures, performed data analytics, and assessed the operating effectiveness of the change management process.

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 change management requires improvement in the design and operation of some control activities.

RISK OBSERVATION SUMMARY

The table below summarizes the risk observations identified during the course of the audit, grouped by the associated risk factor as 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. System Configuration Risk	🔴	🟡	🔴
2.1 Post-Implementation Review 2.2 Change Management Metrics 2.3 Change Reconciliation			
3. Segregation of Duties Risk	🔴	🔴	🔴
3.1 Production Migration			
4. Compliance Risk	🔴	🟡	🔴
4.1 Data Integrity 4.2 Testing			

The risk observations and management's risk mitigation strategies are discussed in detail in the attached document. Internal Audit will conduct a follow-up review at a later date 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
Deputy County Manager/Chief of Staff
Assistant County Managers
Deputy County Attorney
Senior County Attorney
Board of County Commissioners
Audit Review Committee

BACKGROUND

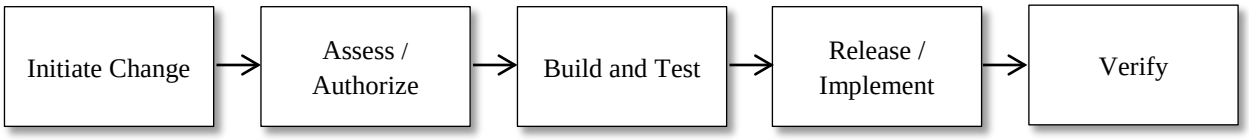
An information technology (IT) environment must constantly adapt in response to changing business needs and the introduction and availability of new technologies. Therefore, organizations require a disciplined process to introduce required changes with minimal disruption to activities that support the achievement of organizational goals and objectives.

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

Change Management

Change management is a process designed to manage, document, and implement approved changes into the IT production environment. A good change management process limits the risks associated with the introduction of new elements and other modifications into the IT environment to prevent unapproved changes and to rapidly recover from change-related problems. Figure 1 depicts the phases of a simplified change management process.

Figure 1: Change Management Workflow



The production environment is where the programs that run an organization are executed, which includes the personnel, processes, data, hardware, and software needed to perform day-to-day operations.

A change management event represents any modification to a configuration item, such as an addition or removal of hardware, software, applications, or systems in the IT production environment. All changes to the production environment require a change request, which is used to record modifications within the production environment.

The Department has a pre-defined change process model that defines the necessary tasks to manage changes, using the following categories:

- *Standard*—Changes that are low risk, segmented, isolated, pre-approved, frequently occurring in the production environment
- *Normal*—By default, all changes are considered normal unless the change conforms to the categories of "Standard" or "Emergency"
- *Emergency*—Changes that require immediate action

Table 1 – Change Type and Number

Changes (November 2013 through August 15, 2014)			Status					
Change Type	**Changes**		**Closed/Completed**		**Implementing**		**New**	
Standard Change	509	85%	506	85%	3	75%	0	0%
Normal Change	69	11%	67	11%	1	25%	1	100%
Emergency Change	24	4%	24	4%	0	0%	0	0%
Totals	**602**	**100%**	**597**	**100%**	4	**100%**	**1**	**100%**

Auditor Analysis, Information Technology Service Management data, unaudited

Roles and Responsibilities

The Department has defined primary roles in the change management process, each with separate and distinct responsibilities.

- Change Requester—Initially perceives the need for the change and initiates a change request
- Change Manager—Oversees the change management process and chairs the Change Advisory Board
- Change Advisory Board (CAB)—The internal consultative body that reviews and approves changes and assists in the assessment and prioritization of changes
    - Emergency Change Advisory Board (ECAB), a subset of the CAB, reviews and approves all emergency changes
- Change Implementer—The requester's representative or proxy who manages the change from initiation to close

Change Management System

The Department employs Cherwell, an information technology service management system, which manages changes to the production environment. Cherwell provides the ability to track the status of change requests throughout the change management process, including details about the deployment of the change.

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 Observation

1.1 Formal Documentation—While the Department has formal, documented policies and procedures for some aspects of its change management process, they did not reflect current and leading 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.

Affected change management activities include, but are not necessarily limited to:

- Segregation of duties
- Risk assessment and impact analysis
- Roles and responsibilities
- Metrics and management reporting requirements
- Relationship with other IT processes
- Workflow phases, deliverables, and document retention requirements
- Monitoring and auditing requirements

Recommendation

1.1 Internal Audit recommends management update its Change Management Standard Operating Procedures to incorporate relevant details regarding:

- Segregation of duties for all IT staff involved in the change management process
- Guidance and criteria for risk assessment and impact analysis, including security, capacity, and performance implications
- Roles and responsibilities of business users and all IT staff in the areas of change submission, building, testing, and implementation
- Performance analysis metrics and management reporting data
- The relationship of change management with other key IT business processes, such as system development life cycle activities and incident, configuration, and release management
- Change management workflow phases that manage change design, development, testing and implementation, phase deliverables, and related documentation retention requirements
- Change management monitoring and auditing requirements

Management's Risk Mitigation Strategy

1.1 The Change Management SOP (Standard Operating Procedure) is based on Cisco Change Management and ITIL Service Management and will be updated to reflect the necessary changes by the end of Q2 FY16. However, some of the recommendations had already been implemented prior to the report coming out. The performance analysis metrics and management reporting data are a function of the Cherwell system itself and hopefully will be addressed when the system is enhanced, sometime in Q3 or Q4 FY16.

Risk Factor	Criticality	Design	Operation
2. System Configuration Risk	🔴	🟡	🔴

Risk Observations

2.1 Post-Implementation Review—The Department did not conduct a post-implementation review to confirm changes implemented into the production environment met their objectives with no unexpected side effects, and that results met stakeholder expectations. Further, the review could provide information to improve the change management process in the future.

2.2 Change Management Metrics—The Department did not identify or report on key change management metrics to measure the effectiveness of the change management process. As a result, management has limited assurance change management activities are performing as expected.

2.3 Change Reconciliation—The Department did not reconcile implemented changes into the production environment against authorized changes to prevent or timely detect variances or unauthorized changes.

Recommendations

2.1 Internal Audit recommends management conduct independent post-implementation reviews of changes implemented into the production environment. Any issues identified in the review should be documented and reported on the extent to which:

- Business requirements were met
- Internal and external stakeholders' expectations were met
- Unexpected impacts on the organization occurred
- Key risks were mitigated
- Change management processes were performed effectively and efficiently

2.2 Internal Audit recommends management define and establish key change management metrics, such as number of changes by category, number of successful/failed changes as percentage of actual changes made, and percentage of time spent on unplanned work.

2.3 Internal Audit recommends management routinely reconcile authorized changes against implemented changes and investigate any variances. The reconciliations should be documented, independently reviewed, and retained for future reference.

Management's Risk Mitigation Strategy

2.1 A post-implementation review is being addressed in the beginning of Q2 FY16.

2.2 Some of the recommended reports are already available within the ITSM system and KPI's will be discussed for approval in Q2 FY16.

2.3 Currently, there is no automated mechanism to formally and adequately detect unauthorized changes. Discussions to purchase hardware and/or software to detect unauthorized change will occur in Q4 FY16.

Risk Factor	Criticality	Design	Operation
3. Segregation of Duties Risk	🔴	🔴	🔴

Risk Observation

3.1 Production Migration—Programmers who develop or modify configuration items also have the ability to access and migrate changes into the production environment, which could lead to unauthorized changes.

Recommendation

3.1 Internal Audit recommends management appropriately segregate the duties for development, modification, and migration of configuration items into the production environment. If that is not possible, management should implement appropriate compensating controls.

Management's Risk Mitigation Strategy

3.1 This is not a function of the Change Manager but segregation of duties within the programming department has been implemented and, with the addition of the Quality Assurance (QA) group (newly created group), this will be slowly rolled out as the team is built. A limited set of applications are being addressed starting in Q1 FY16 and increasing as the QA group is built out.

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

Risk Observations

4.1 Data Integrity—Certain data maintained in Cherwell was inaccurate or incomplete. Seven of 602 changes or 1% had completion dates earlier than the start dates. Nineteen of 602 or 3 % closed change records did not have a close date, 17 of which did not have a completion status code. As a result, the data did not provide an accurate reflection of change management activities, nor was it in compliance with the Department's Change Management Standard Operating Procedures.

4.2 Testing—Beyond notations in Cherwell, 64 of 69 or 93% of normal changes sampled did not evidence that testing was conducted prior to migration into the production environment. Failure to

document and retain evidence that testing was conducted increases the risk that errors will be migrated into the production environment.

Recommendations

4.1 Internal Audit recommends management ensure changes recorded in Cherwell comply with Change Management Standard Operating Procedures.

4.2 Internal Audit recommends management ensure all change management testing activities are documented and retained.

Management's Risk Mitigation Strategy

4.1 The SOP will be updated with the recommendation to have effective and enforced consequences for not following proper Change Control procedures. This will be documented in Q2 FY16.

4.2 The new QA group will be leading this initiative and has already started working with development on a limited number of high profile applications. This will continue to expand as the QA group is built out. This was started in Q1 FY16 and will continue to expand throughout the year.

APPENDIX A − Risk Factor Definitions

Risk Factor	Definition
Policies and Procedures Risk	Policies and procedures that are non-existent, ineffective, unclear, or outdated may result in poorly executed processes and increased operating costs.
System Configuration Risk	Lack of effective configuration management processes may result in systems that do not perform as intended to support operation of critical processes.
Segregation of Duties Risk	Inadequate segregation of duties may allow individuals to carry out inappropriate activities without timely detection.
Compliance Risk	Lack of compliance with established policies, procedures, regulations, and/or statutory requirements may result in unacceptable performance that affects financial, operational, and/or customer objectives.

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 adequacy 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.