

LOS ANGELES COUNTY AUDITOR-CONTROLLER

Arlene Barrera
AUDITOR-CONTROLLER

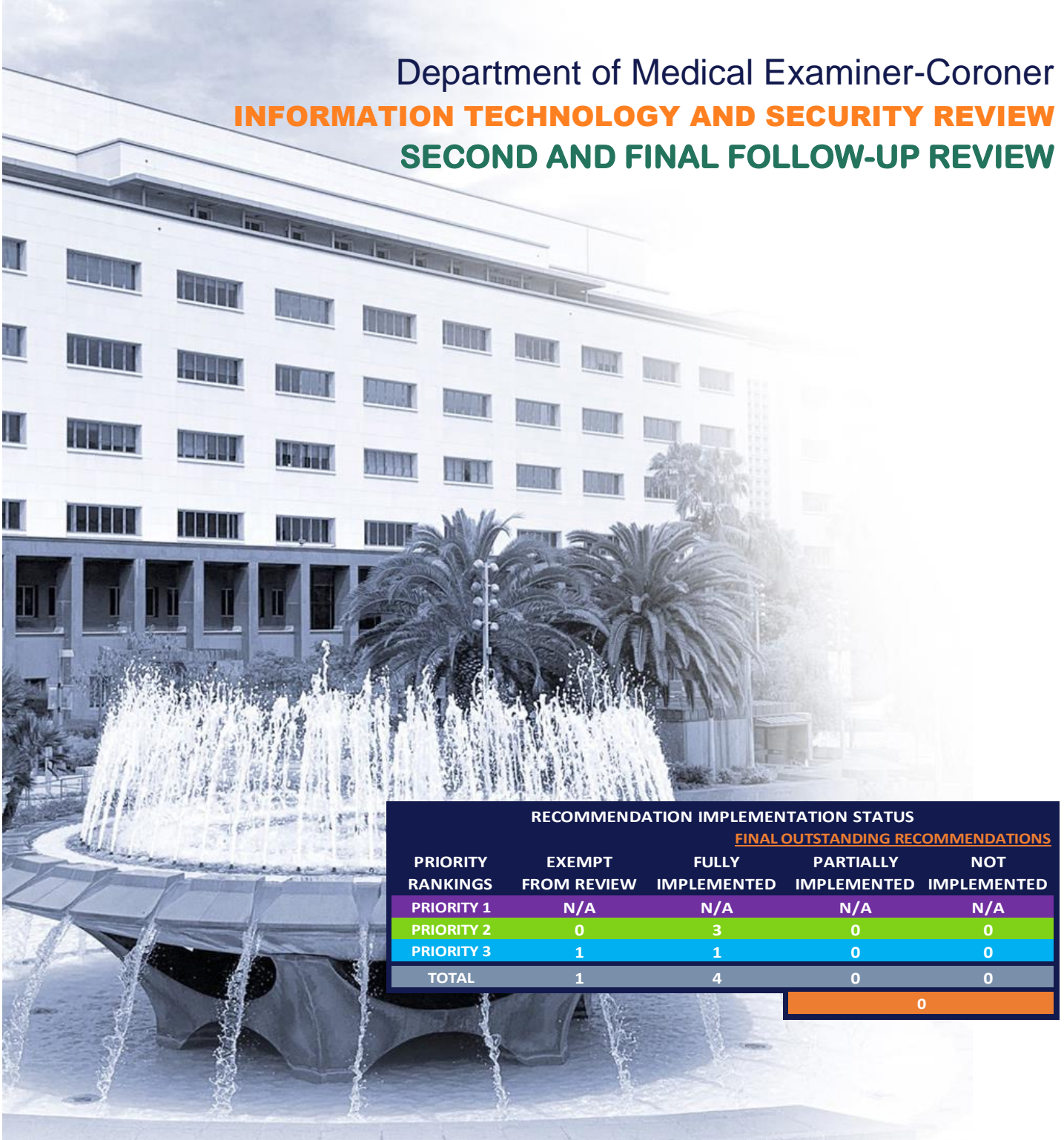
Peter Hughes
ASSISTANT AUDITOR-CONTROLLER

Mike Pirolo
DIVISION CHIEF

AUDIT DIVISION

November 15, 2019

Department of Medical Examiner-Coroner **INFORMATION TECHNOLOGY AND SECURITY REVIEW** **SECOND AND FINAL FOLLOW-UP REVIEW**



RECOMMENDATION IMPLEMENTATION STATUS				
FINAL OUTSTANDING RECOMMENDATIONS				
PRIORITY RANKINGS	EXEMPT FROM REVIEW	FULLY IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED
PRIORITY 1	N/A	N/A	N/A	N/A
PRIORITY 2	0	3	0	0
PRIORITY 3	1	1	0	0
TOTAL	1	4	0	0
				0



BOARD OF SUPERVISORS

Hilda L. Solis
FIRST DISTRICT

Mark Ridley-Thomas
SECOND DISTRICT

Sheila Kuehl
THIRD DISTRICT

Janice Hahn
FOURTH DISTRICT

Kathryn Barger
FIFTH DISTRICT



ARLENE BARRERA
AUDITOR-CONTROLLER

**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

November 15, 2019

TO: Supervisor Janice Hahn, Chair
Supervisor Hilda L. Solis
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Kathryn Barger

FROM: Arlene Barrera 
Auditor-Controller

SUBJECT: **DEPARTMENT OF MEDICAL EXAMINER-CORONER – INFORMATION
TECHNOLOGY AND SECURITY REVIEW (REPORT #K18BO) –
SECOND AND FINAL FOLLOW-UP REVIEW**

The Auditor-Controller's Audit Division has completed a second and final follow-up review of the Department of Medical Examiner-Coroner – Information Technology and Security Review dated July 26, 2018 (Report #K18BO). The complete follow-up report is attached.

If you have any questions please call me, or your staff may contact Mike Pirolo at (213) 253-0100.

AB:PH:MP

Attachment (Report #K20CD)

c: Sachi A. Hamai, Chief Executive Officer
Jonathan R. Lucas, M.D., Chief Medical Examiner-Coroner
William S. Kehoe, Chief Information Officer, Chief Executive Office
Ralph Johnson, Chief Information Security Officer, Chief Executive Office
Audit Committee
Countywide Communications

*Help Conserve Paper – Print Double-Sided
"To Enrich Lives Through Effective and Caring Service"*



BE COUNTED ✓

<http://census.lacounty.gov>



ARLENE BARRERA
AUDITOR-CONTROLLER


**COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER**

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

ADDRESS ALL CORRESPONDENCE TO:
AUDIT DIVISION
350 S. FIGUEROA ST., 8th FLOOR
LOS ANGELES, CA 90071-1304

November 15, 2019

TO: Jonathan R. Lucas, M.D., Chief Medical Examiner-Coroner
Department of Medical Examiner-Coroner

FROM: Dr. Peter Hughes 
Assistant Auditor-Controller

Mike Pirolo, Division Chief 
Audit Division

**SUBJECT: DEPARTMENT OF MEDICAL EXAMINER-CORONER – INFORMATION
TECHNOLOGY AND SECURITY REVIEW (REPORT #K18BO) –
SECOND AND FINAL FOLLOW-UP REVIEW**

We have conducted a second and final follow-up review of the Department of Medical Examiner-Coroner (DMEC or Department) Information Technology and Security Review dated July 26, 2018 (Report #K18BO). On June 17, 2019, we reported on the implementation status of the 15 recommendations in the report. See Table 1 for a recap of the results of our first follow-up review.

For this second follow-up, we reviewed the status of three Priority 2 and one Priority 3 recommendations, as requested by the Audit Committee, that had not been fully implemented at the time of our first follow-up review. See Table 2 for a summary of the status of corrective action for these recommendations based on our review of relevant supporting documentation provided by the Department.

Help Conserve Paper – Print Double-Sided
“To Enrich Lives Through Effective and Caring Service”



BE COUNTED ✓

<http://census.lacounty.gov>

Table 1 – Results of First Follow-up Review

PRIORITY RANKINGS	TOTAL RECOS	RECOMMENDATION IMPLEMENTATION STATUS		
		FULLY IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED
PRIORITY 1	9	9	0	0
PRIORITY 2	4	1	3	0
PRIORITY 3	2	0	2	0
TOTAL	15	10	5	0
				5

Table 2 - Results of Second and Final Follow-up Review

PRIORITY RANKINGS	TOTAL RECOS OUTSTANDING ¹	EXEMPT FROM REVIEW ²	RECOMMENDATION IMPLEMENTATION STATUS		
			FULLY IMPLEMENTED	PARTIALLY IMPLEMENTED	NOT IMPLEMENTED
PRIORITY 1	N/A	N/A	N/A	N/A	N/A
PRIORITY 2	3	0	3	0	0
PRIORITY 3	2	1	1	0	0
TOTAL	5	1	4	0	0
				0	

The Department fully implemented all four recommendations from this follow-up review to enhance their processes for user access controls, IT equipment disposition, IT risk assessment, and physical security. Attachment I provides details of our review and the Department's actions to implement corrective action. Definitions of the Priority Rankings are included in Attachment II.

Follow-up Process

Board of Supervisors Policy 4.050 requires the Auditor-Controller (A-C) to follow up with departments to ensure they have taken corrective action to address audit recommendations. To assist the A-C in accomplishing this task, six months after an audit report is issued, departments must provide the A-C's Audit Division a *Corrective Action Implementation Report (CAiR)* that provides a detailed status of corrective action(s) taken to implement each recommendation in the report. For recommendations reported as implemented, departments must attach documentation to the CAiR that demonstrates the corrective action taken.

¹ "Total outstanding" refers to recommendations noted as "Partially Implemented" or "Not Implemented" in our first follow-up report issued June 17, 2019.

² In accordance with our standard procedures, we follow-up on Priority 3 recommendations at the Audit Committee's request. The Audit Committee requested that we follow-up on one of the two Priority 3 recommendations. As a result, the other recommendation is exempt from review.

Jonathan R. Lucas, M.D.

November 15, 2019

Page 3

Our review consisted of an examination of DMEC's description of actions taken per the CAiR, the relevant documents and supporting evidence provided by the Department, as well as inquiry and discussion with responsible departmental personnel. Our follow-up review did not constitute an "audit" and did not include a sampling of transactions for testing and verification purposes.

We thank DMEC management and staff for their cooperation and assistance during our review. If you have any questions, please call Mike Pirolo at (213) 253-0100.

PH:MP:JO:rs

Attachments

c: Arlene Barrera, Auditor-Controller

DEPARTMENT OF MEDICAL EXAMINER-CORONER
INFORMATION TECHNOLOGY AND SECURITY REVIEW (REPORT #K18BO)
SECOND AND FINAL FOLLOW-UP REVIEW

No.	RECOMMENDATION	PRIORITY	STATUS (1)	A-C COMMENTS
10	<p>Department of Medical Examiner-Coroner (DMEC or Department) management establish a process to periodically review network and Case Management System (CME) user access rights to ensure all access is authorized and consistent with users' job duties.</p> <p>Original Issue/Impact: DMEC did not have a process to periodically review network and CME user access rights to ensure all access is authorized and appropriate. As a result, inappropriate access to sensitive decedent data could occur without timely detection.</p>	2	I	<p>We confirmed DMEC established a process to conduct quarterly user access reviews for their network and CME by reviewing the Department's user access review procedures. We also confirmed DMEC completed user access reviews by reviewing the Department's August 2019 review results.</p>
12	<p>DMEC management develop ongoing self-monitoring processes that include:</p> <ul style="list-style-type: none"> a) Examination of process/control activities, such as review of an adequate number of transactions on a regular basis to ensure adherence to Board of Supervisors Policies (Board Policies) and applicable County Information Technology (IT) standards. b) Documenting the monitoring activity and retaining evidence so it can be subsequently validated. 	2	I	<p>We confirmed DMEC management established self-monitoring processes for IT equipment disposition, employee IT AUA policy acknowledgments, and building physical access controls by reviewing the Department's monitoring procedures for each area.</p> <p>The Department's self-monitoring processes require staff to periodically sample and verify compliance with Board Policies and elevate material exceptions timely to ensure corrective actions are implemented. The Department indicated it plans to begin monitoring in January 2020 to best align with several control activities that occur in December (e.g., year-end physical inventory count).</p>

Footnotes

(1) Status definitions:

"I" indicates the department has fully implemented corrective action that is responsive to the recommendation.

"PI" indicates the department has partially implemented corrective action that is responsive to the recommendation.

"NI" indicates the department has not implemented corrective action that is responsive to the recommendation.

No.	RECOMMENDATION	PRIORITY	STATUS (1)	A-C COMMENTS
	<p>c) Elevating material exceptions to management on a timely basis to ensure awareness of relative control risk and to ensure appropriate corrective actions are implemented.</p> <p>Original Issue/Impact: DMEC did not have a process to conduct ongoing self-monitoring for their IT equipment disposition process, staff Acceptable Use Agreement (AUA) policy acknowledgments, and building access controls. This prevents DMEC management from ensuring they achieve important Departmental and County IT and security objectives, and increases the risk for noncompliance with County IT and security rules.</p>			
13	<p>DMEC management establish a process to conduct IT risk assessments and for management to monitor and document that the risk assessment process is working effectively.</p> <p>Original Issue/Impact: DMEC did not have a process to conduct risk assessments of their IT resources, including 350 desktop/laptop computers and two critical IT systems that maintain sensitive decedent data. As a result, DMEC may not identify IT security threats and vulnerabilities timely and develop corrective action plans.</p>	2	I	<p>We confirmed DMEC management established a process to conduct, and for management to monitor, IT risk assessments by reviewing the Department's IT risk assessment procedures. We also confirmed staff adhere to the IT risk assessment process by reviewing the Department's August 2019 IT risk assessment and monitoring activities.</p>
14	<p>DMEC management evaluate implementing a keycard access system and/or installing keypad locks to secure access to confidential areas.</p>	3	I	<p>We confirmed DMEC solicited a vendor to evaluate implementing a keycard access system throughout the Department's three offices by reviewing the vendor's September 2019 cost estimate, work proposal for equipment, and technical support. The department's</p>

Footnotes

(1) Status definitions:

"I" indicates the department has fully implemented corrective action that is responsive to the recommendation.

"PI" indicates the department has partially implemented corrective action that is responsive to the recommendation.

"NI" indicates the department has not implemented corrective action that is responsive to the recommendation.

No.	RECOMMENDATION	PRIORITY	STATUS (1)	A-C COMMENTS
	<p>Original Issue/Impact: We noted DMEC's 248 staff may need several different physical keys to access various areas of DMEC's three offices. The large number of physical keys in use makes it difficult to manage key assignments. This increases the risk for the loss, theft, and/or unauthorized copying of keys, which can lead to inappropriate access to DMEC assets and sensitive decedent data.</p>			<p>management indicated they plan to include the key card system cost estimate in their Fiscal Year 2020-21 funding request to the Chief Executive Office in January 2020.</p>

Footnotes

(1) Status definitions:

"I" indicates the department has fully implemented corrective action that is responsive to the recommendation.

"PI" indicates the department has partially implemented corrective action that is responsive to the recommendation.

"NI" indicates the department has not implemented corrective action that is responsive to the recommendation.

PRIORITY RANKING DEFINITIONS

Auditors use professional judgment to assign rankings to recommendations using the criteria and definitions listed below. The purpose of the rankings is to highlight the relative importance of some recommendations over others based on the likelihood of adverse impacts if corrective action is not taken and the seriousness of the adverse impact. Adverse impacts are situations that have or could potentially undermine or hinder the following:

- a) The quality of services departments provide to the community,
- b) The accuracy and completeness of County books, records, or reports,
- c) The safeguarding of County assets,
- d) The County's compliance with pertinent rules, regulations, or laws,
- e) The achievement of critical programmatic objectives or program outcomes, and/or
- f) The cost-effective and efficient use of resources.

Priority 1 Issues

Priority 1 issues are control weaknesses or compliance lapses that are significant enough to warrant immediate corrective action. Priority 1 recommendations may result from weaknesses in the design or absence of an essential procedure or control, or when personnel fail to adhere to the procedure or control. These may be reoccurring or one-time lapses. Issues in this category may be situations that create actual or potential hindrances to the department's ability to provide quality services to the community, and/or present significant financial, reputational, business, compliance, or safety exposures. Priority 1 recommendations require management's immediate attention and corrective action within 90 days of report issuance, or less if so directed by the Auditor-Controller or the Audit Committee.

Priority 2 Issues

Priority 2 issues are control weaknesses or compliance lapses that are of a serious nature and warrant prompt corrective action. Priority 2 recommendations may result from weaknesses in the design or absence of an essential procedure or control, or when personnel fail to adhere to the procedure or control. These may be reoccurring or one-time lapses. Issues in this category, if not corrected, typically present increasing exposure to financial losses and missed business objectives. Priority 2 recommendations require management's prompt attention and corrective action within 120 days of report issuance, or less if so directed by the Auditor-Controller or the Audit Committee.

Priority 3 Issues

Priority 3 issues are the more common and routine control weaknesses or compliance lapses that warrant timely corrective action. Priority 3 recommendations may result from weaknesses in the design or absence of a procedure or control, or when personnel fail to adhere to the procedure or control. The issues, while less serious than a higher-level category, are nevertheless important to the integrity of the department's operations and must be corrected or more serious exposures could result. Departments must implement Priority 3 recommendations within 180 days of report issuance, or less if so directed by the Auditor-Controller or the Audit Committee.