University of California
2019 Ethics, Compliance and Audit Symposium

REACHING NEW HEIGHTS

Best Practices for Audit Follow-up

Matt Hicks, Systemwide Deputy Audit Officer, UCOP

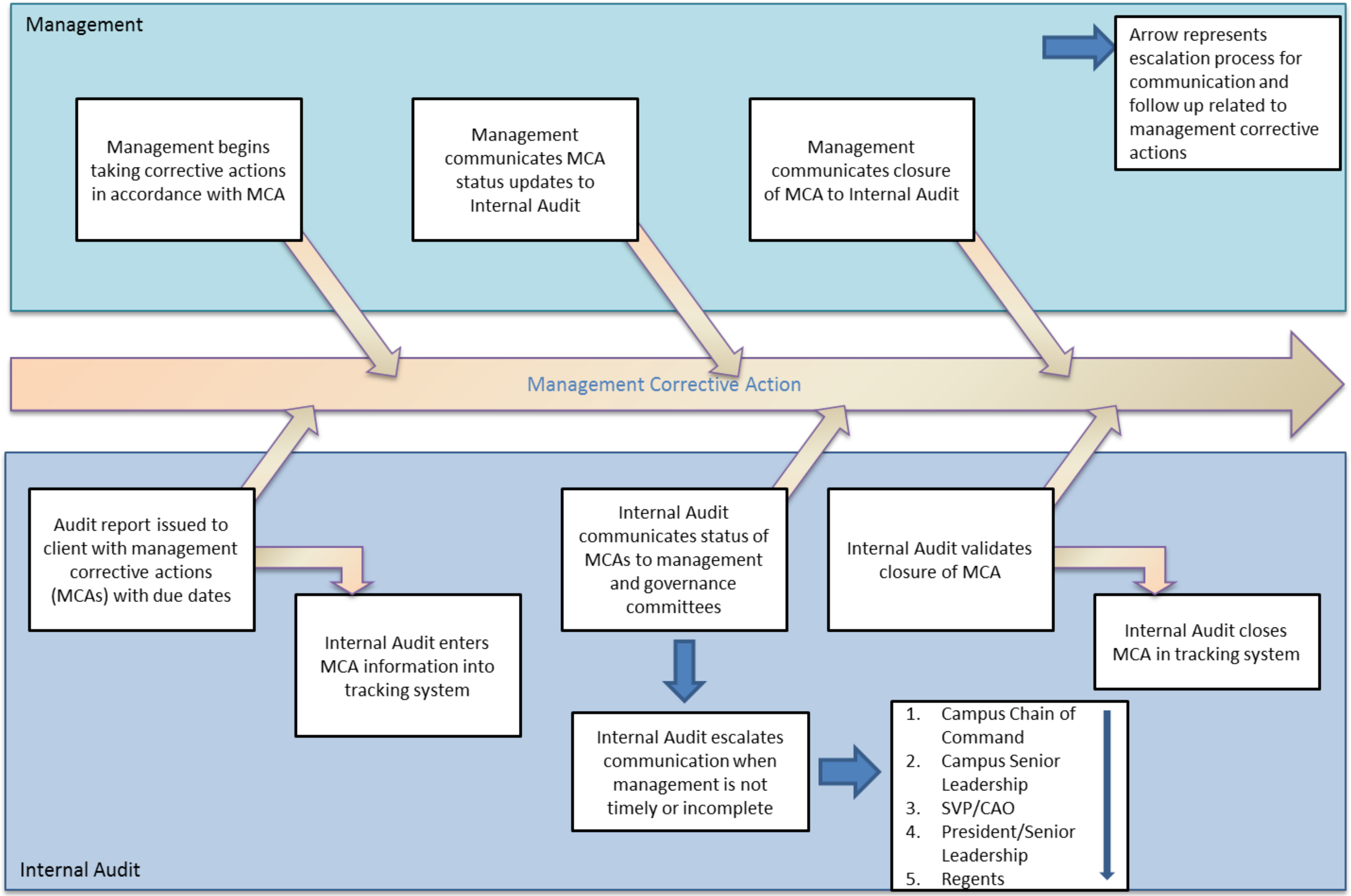
Loran Lerma, Principal Auditor, UC Irvine

Greg Loge, Systemwide Cybersecurity Audit Director, UCOP

Agenda

1. UC Audit Follow-Up Procedures
2. IIA and UC Guidance on Audit Follow-Up
   - Management Risk Acceptance
3. TeamMate Reporting and Wrap Up Procedures
4. Cybersecurity Audit Team (CAT) Audit Follow-Up
5. 300+ MCAs Success Story – UC Irvine

Audit Follow-up Process



Management

Management begins taking corrective actions in accordance with MCA

Management communicates MCA status updates to Internal Audit

Management communicates closure of MCA to Internal Audit

Arrow represents escalation process for communication and follow up related to management corrective actions

Management Corrective Action

Audit report issued to client with management corrective actions (MCAs) with due dates

Internal Audit enters MCA information into tracking system

Internal Audit communicates status of MCAs to management and governance committees

Internal Audit escalates communication when management is not timely or incomplete

1. Campus Chain of Command
2. Campus Senior Leadership
3. SVP/CAO
4. President/Senior Leadership
5. Regents

Internal Audit validates closure of MCA

Internal Audit closes MCA in tracking system

Internal Audit

IIA Standards on Audit Follow-up

2500 – Monitoring Progress

The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2500.A1 – The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2500.C1 – The internal audit activity must monitor the disposition of results of consulting engagements to the extent agreed upon with the client.

Practice Advisory 2500.A1-1: Follow-up Process

- Internal auditors determine whether management has taken action or implemented the recommendation
- Follow-up is a process by which internal auditors evaluate the adequacy, effectiveness, and timeliness of actions taken by management on reported observations and recommendations
  - This process also includes determining whether senior management and/or the board have assumed the risk of not taking corrective action on reported observations.
- The internal audit activity's charter should define the responsibility for follow-up
  - The chief audit executive (CAE) determines the nature, timing, and extent of follow-up

Practice Advisory 2500.A1-1: Follow-up Process

- The CAE is responsible for scheduling follow-up activities as part of developing engagement work schedules
- Where the CAE judges that management's oral or written response indicates that action taken is sufficient when weighed against the relative importance of the observation or recommendation, internal auditors may follow up as part of the next engagement
- Internal auditors ascertain whether actions taken on observations and recommendations remedy the underlying conditions
  - Follow-up activities should be appropriately documented

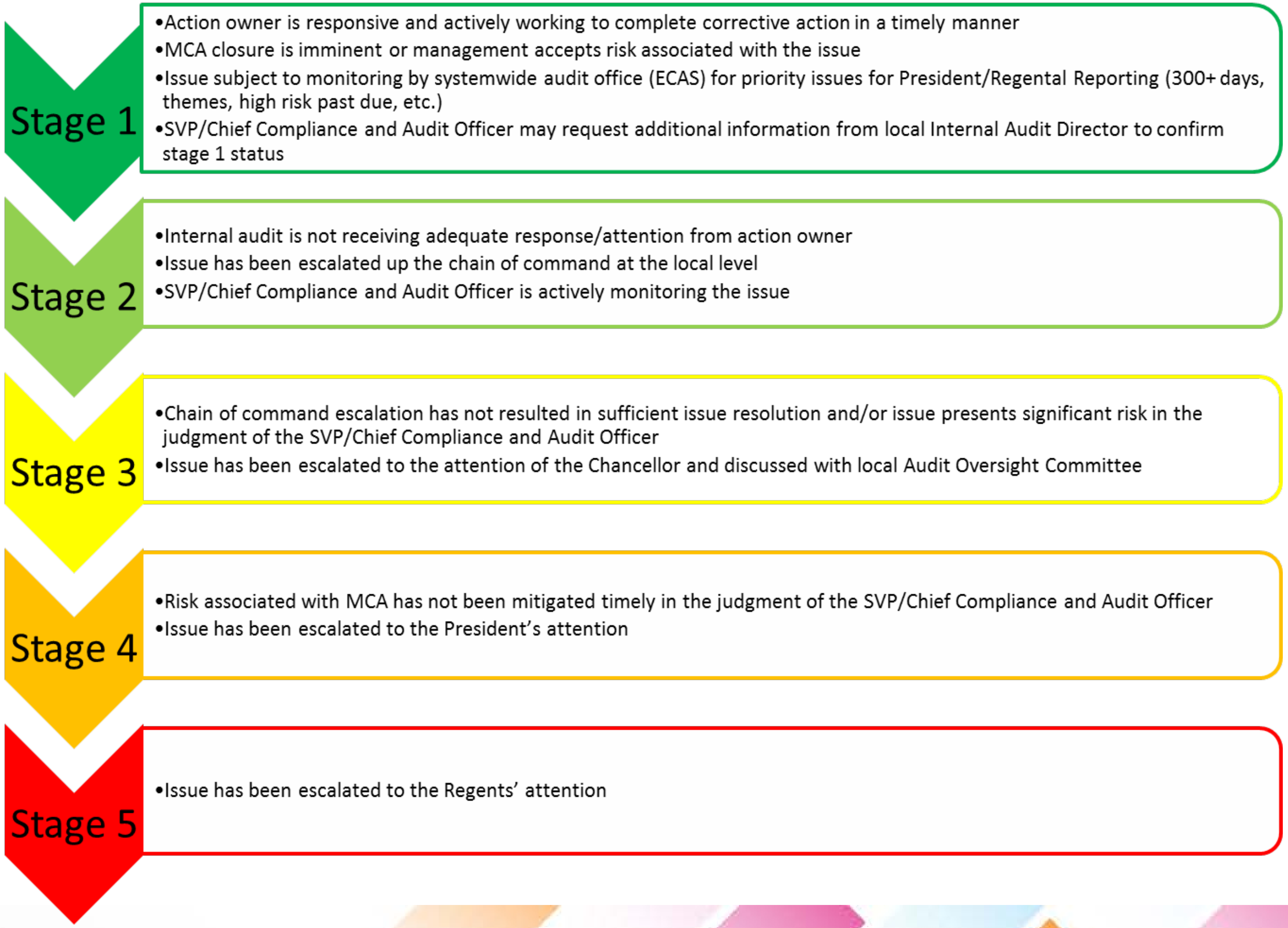
Internal Audit Manual on Audit Follow-up (Section 6400)

- TeamCentral should be used to track and manage audit findings and corresponding management corrective actions
  - May be supplemented as necessary on a local basis to meet local management reporting expectations
- Auditor should follow up on MCAs on a timely basis using his/her professional judgment to:
  - Ascertain status of MCA and evaluate the adequacy, progress and timeliness of actions taken
  - Decide whether there is need for additional testing/follow-up
  - Document the results of follow-up in TeamCentral

Internal Audit Manual on Audit Follow-up (Section 6400)

- Internal Audit determines if the risk identified was resolved or if management has assumed the risk of not taking action
- Where recommendations are provided, management has the option to consider other action as long as the risk is resolved and/or managed to an acceptable level
- Audit management should notify the next higher level of line management and/or the audit oversight committee of any unsatisfactory or untimely responses or actions
- IAD should periodically advise the audit oversight committee of follow-up activities, high risk open items and MCAs that are overdue
- If management is not taking appropriate or timely action to complete and MCA, the issue will be escalated

MCA Escalation Stages



Stage 1

- Action owner is responsive and actively working to complete corrective action in a timely manner
- MCA closure is imminent or management accepts risk associated with the issue
- Issue subject to monitoring by systemwide audit office (ECAS) for priority issues for President/Regental Reporting (300+ days, themes, high risk past due, etc.)
- SVP/Chief Compliance and Audit Officer may request additional information from local Internal Audit Director to confirm stage 1 status

Stage 2

- Internal audit is not receiving adequate response/attention from action owner
- Issue has been escalated up the chain of command at the local level
- SVP/Chief Compliance and Audit Officer is actively monitoring the issue

Stage 3

- Chain of command escalation has not resulted in sufficient issue resolution and/or issue presents significant risk in the judgment of the SVP/Chief Compliance and Audit Officer
- Issue has been escalated to the attention of the Chancellor and discussed with local Audit Oversight Committee

Stage 4

- Risk associated with MCA has not been mitigated timely in the judgment of the SVP/Chief Compliance and Audit Officer
- Issue has been escalated to the President's attention

Stage 5

- Issue has been escalated to the Regents' attention

Management Risk Acceptance

- IIA Standards:
  - 2600 – Communicating the Acceptance of Risks
    - When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.
  - Interpretation: The identification of risk accepted by management may be observed through an assurance or consulting engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means. It is not the responsibility of the chief audit executive to resolve the risk.

Management Risk Acceptance

- UC Audit Manual:
  - 6300 Reporting Results
    - Internal Audit obtains agreement with the engagement client about the conclusions and action plans of the audit. In the event of a disagreement, the communications state both positions and the reasons for the disagreement.

TeamMate Reporting and Wrap Up Procedures

- Complete Lead Auditor wrap-up procedures
- Complete Manager wrap-up procedures
- Complete Administrator (QAR) steps

TeamMate Reporting and Wrap Up Procedures

Lead Auditor

1. Add final audit report copy (.pdf) to EWP
2. In EWP, create procedure step for all reported exceptions
3. From the final report copy Word.doc, cut/paste observations and MCAs into EWP exceptions in same order as report (so EWP exception #1 matches the final report #1) and enter:
   - Exception Title
   - Type (Operational, Financial, Compliance)
   - Level (Report issue)

TeamMate Reporting and Wrap Up Procedures

<u>Lead Auditor</u>

3. Complete Tabs:
    - Finding (verbatim as in report final)
    - Brief Summary (summary of observation) ** Important/used by Matt H.to report to Regent’s Audit Committee
    - Properties (VC Code, Location, COSO Code, Finding Index Code (same as Origin code in Profile/General Tab)
    - Recommendation (Title)
    - MCA (verbatim as in report final)
    - Implementation (Estimated date, Track in TeamCentral checked)
    - Contact(s) - Owner: Responsible person/MCA owner – First/Last name and email
    - Brief MCA (summary of MCA) ** Important/used by Matt H. to report to Regent’s Audit Committee
    - Properties - Findings Risk Rating (High, Medium, Low)
    - State (Open)

TeamMate Reporting and Wrap Up Procedures

Lead Auditor

4. Run UC Mandatory Data Elements Validation Checklist

A red highlighted field or value in the Validation Checklist report indicates that a required data element is invalid or is not completed. A yellow highlighted field or value indicates the status of an optional data element. The Validation Checklist report should be re-run until all of the mandatory UC data elements are completed and the required values in the report appear highlighted green.

TeamMate Reporting and Wrap Up Procedures

Manager

1. In the Profile Tab Complete:
   - Team Tab – Access and Coordinators - Add New for both Project Access Groups and Implementation Coordinator Group – enter UCI IC Group
   - Schedule Tab – Actual End Date
   - Status and Milestones Tab – Status Tab: Actual Dates, Milestones Tab: Fieldwork Completion date, Draft Report date, Final Report Issued date
2. Select TeamCentral (Opens TeamCentral Send Wizard)
3. Filter exceptions to send (Limit to levels: Report Issue)
4. Select Finish – Obtain confirmation
5. Open TeamMate Central and validate/confirm proper send to central

TeamMate Reporting and Wrap Up Procedures

Administrator

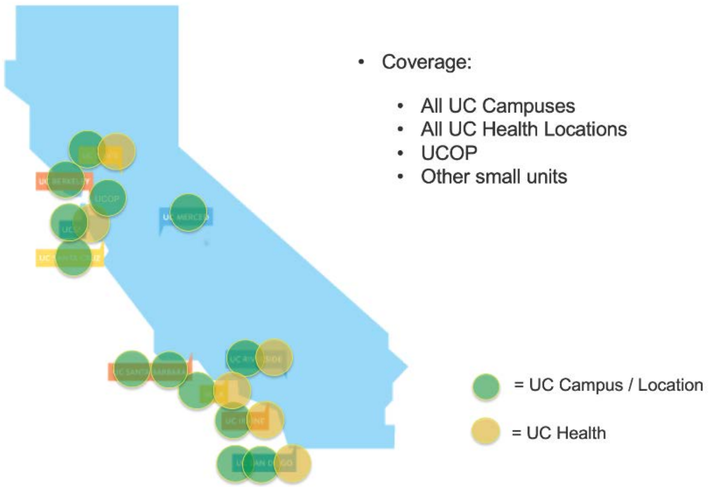
1. Open EWP file and ensure:
   - Final report added (.pdf)
   - All draft reports removed
   - All workpapers signed-off by preparer/reviewer
   - Attestations prepared/signed-off
   - Coaching notes have been removed
   - Extraneous workpapers have been removed
2. Send Survey to Auditee

CAT Audit Follow-Up

- Background - Cybersecurity Audit Team (CAT)
  - Team Focus
    - Support location internal audit offices as needed with cybersecurity expertise
    - Systemwide cyber-risk focused internal audits projects
  - Systemwide Audit Projects
    - Performed all across UC system
    - Reports and associated management corrective actions (MCAs) issued to each location

CAT Audit Follow-Up - Example

- Example Audit – FY 17 Vulnerability Assessment and Penetration Testing Audit
  - Performed penetration testing across UC campus locations
  - In first year 56 corrective actions across all UC locations
  - 56 of 56 actions closed on time within 300 day limit
  - MCA focus
    - Strengthen Systems
    - Improve Processes



- Coverage:
  - All UC Campuses
  - All UC Health Locations
  - UCOP
  - Other small units

CAT Audit Follow-Up - Example

- MCA reporting process key to on time closure
  - Monthly MCA reports sent to each location Cyber-Risk Responsible Executive (CRE) and copying the Chief Information Officer (CIO) and Chief Information Security Officer (CISO)
    - Established regular reporting norm – no surprises as deadline approached
    - Easy path for escalation - Leadership informed ongoing of status
    - Monthly report delivery empowered auditors and helped with responsiveness

300+ MCAs Success Story: UC Irvine

- **New Systemwide Audit MCA Reporting Process (October 2018)**

  Regents Compliance and Audit Committee initiated a new process to send reports to the Chancellors on a bi-monthly basis of all MCAs from local internal audit projects that have been open more than 300 days

  Given that these MCAs are reported to the Regents, this process also gives the Chancellors advance notification that these MCAs are being escalated to the Board. Purpose is to increase monitoring of 300+ MCAs status, and determine whether delays or obstacles to closure need further action as necessary

300+ MCAs Success Story: UC Irvine

New UCI Audit MCA Process

At the request of the Chancellor, Vice Chancellor Cortez has initiated a new process to assure that UCI is fully compliant with completing all open MCAs by target deadlines, thus avoiding further actions or escalations.

1. Notification of Incomplete Management Corrective Actions

Senior leadership responsible for administration organizations MCAs will be notified to meet with VC Cortez and IAS to address incomplete MCAs over 100 days old from report date (in order to avoid reaching the 300 day threshold).

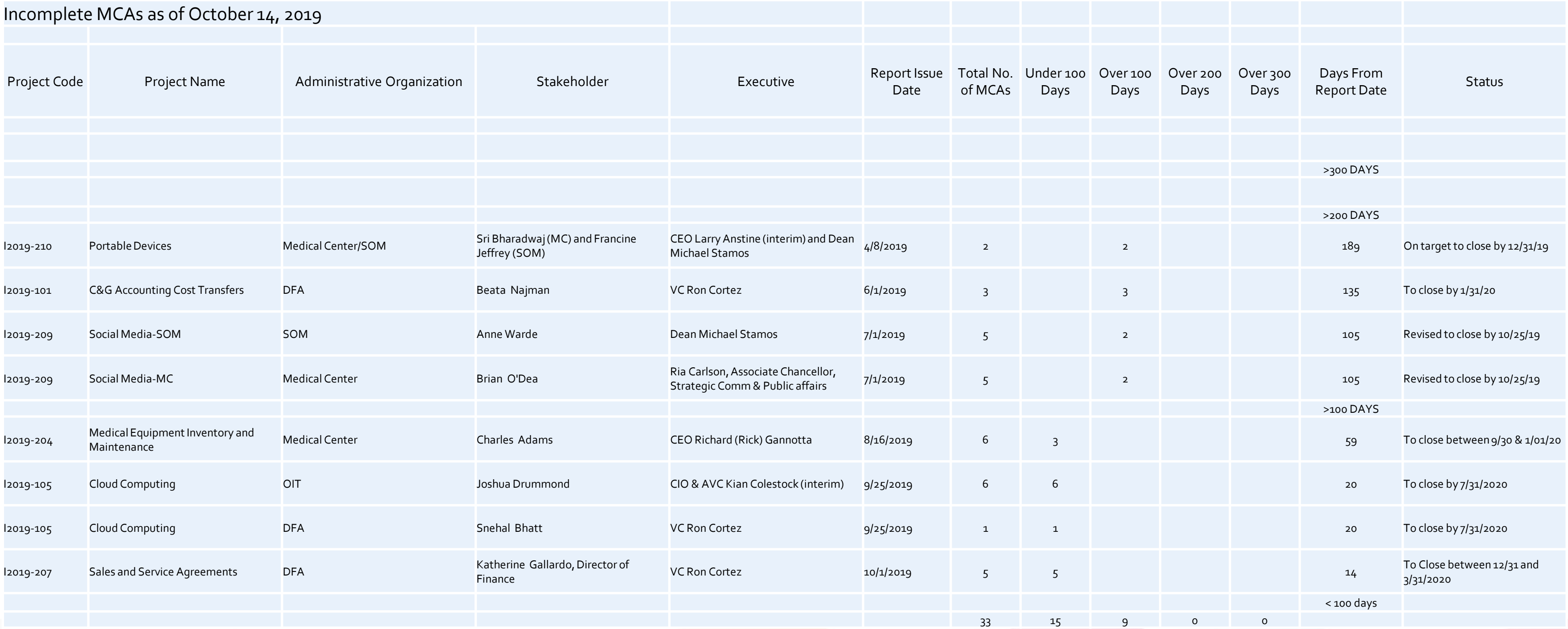
MCAs that require more than 300 days to implement will need to address short term mitigating efforts and or fully explain reasons for the delayed implementation (Regents concern that target dates are not realistic and /or revising the target dates more than once).

2. Progress Report to the Chancellor

VC Cortez will provide a monthly progress report to the Chancellor discussing the status of all incomplete MCAs (especially over 300 days old), and address any concerns that may impede implementation and require further action.

300+ MCAs Success Story: UC Irvine

New UCI Audit MCA Local Report



Incomplete MCAs as of October 14, 2019

Project Code	Project Name	Administrative Organization	Stakeholder	Executive	Report Issue Date	Total No. of MCAs	Under 100 Days	Over 100 Days	Over 200 Days	Over 300 Days	Days From Report Date	Status
											>300 DAYS	
											>200 DAYS	
I2019-210	Portable Devices	Medical Center/SOM	Sri Bharadwaj (MC) and Francine Jeffrey (SOM)	CEO Larry Anstine (interim) and Dean Michael Stamos	4/8/2019	2		2			189	On target to close by 12/31/19
I2019-101	C&G Accounting Cost Transfers	DFA	Beata Najman	VC Ron Cortez	6/1/2019	3		3			135	To close by 1/31/20
I2019-209	Social Media-SOM	SOM	Anne Warde	Dean Michael Stamos	7/1/2019	5		2			105	Revised to close by 10/25/19
I2019-209	Social Media-MC	Medical Center	Brian O'Dea	Ria Carlson, Associate Chancellor, Strategic Comm & Public affairs	7/1/2019	5		2			105	Revised to close by 10/25/19
											>100 DAYS	
I2019-204	Medical Equipment Inventory and Maintenance	Medical Center	Charles Adams	CEO Richard (Rick) Gannotta	8/16/2019	6	3				59	To close between 9/30 & 1/01/20
I2019-105	Cloud Computing	OIT	Joshua Drummond	CIO & AVC Kian Colestock (interim)	9/25/2019	6	6				20	To close by 7/31/2020
I2019-105	Cloud Computing	DFA	Snehal Bhatt	VC Ron Cortez	9/25/2019	1	1				20	To close by 7/31/2020
I2019-207	Sales and Service Agreements	DFA	Katherine Gallardo, Director of Finance	VC Ron Cortez	10/1/2019	5	5				14	To Close between 12/31 and 3/31/2020
											< 100 days	
						33	15	9	0	0		