JUL2023

UCMERCED

INTERNAL AUDIT AND ADVISORY SERVICES

IS-12 Implementation Audit

Report No. M23A004

Internal Audit and Advisory Services Team:
Randy Schwantes, Internal Audit Director
Eduardo Perez Ruiz, Senior Internal Auditor

IS-12 Implementation Audit
Report No. M23A004
July 14, 2023

Distribution List

University of California, Office of the President

Alexander Bustamante	Senior Vice President and Chief Audit and Compliance Officer

Ethics and Compliance Program (ECP) Executive Committee/Audit Committee

Juan Sánchez Muñoz	Chancellor
Marjorie Zatz	Interim Executive Vice Chancellor and Provost
Charles Nies	Vice Chancellor, Student Affairs
Daniel T. Okoli	Vice Chancellor and Chief Operating Officer
Delia Saenz	Vice Chancellor and Chief Diversity Officer
E. Edward Klotzbier	Vice Chancellor, Chief External Relations Officer
Gillian Wilson	Vice Chancellor, Research & Economic Development
Kurt Schnier	Interim Vice Chancellor and Chief Financial Officer
Nick Dugan	Vice Chancellor and Chief Information Officer
Luanna Putney	Associate Chancellor, Chief of Staff
Stella Ngai	Chief Campus Counsel
Viola Kinsman	Chief Ethics & Compliance Officer and Locally Designated Official
Cindi Zimmerman	Risk Manager

University of California, Merced

Jackson Muhirwe	Chief Information Security Officer
Sadie Johnson	Business Continuity Planner
Nick Hansard	Director, Cloud Services

IS-12 Implementation Audit

EXECUTIVE SUMMARY

Internal Audit and Advisory Services (Internal Audit) has conducted an audit of IT Recovery at UC Merced. This audit was performed in accordance with Internal Audit's fiscal year 2023 audit plan. The primary objective of the audit was to evaluate processes and controls in place to facilitate compliance with University of California (UC) Policy IS-12: *IT Recovery* (IS-12) requirements.

The Office of Information Technology (OIT) has adopted an iterative approach to compliance with IS-12 and has made efforts to reach a compliance state. However, Internal Audit noted instances of control weaknesses that need improvement in order to provide reasonable assurance that risks are being mitigated and objectives are being met.

The following observations need improvement to strengthen internal controls and/or effect compliance:

Business Impact Analysis. Internal Audit Recommends Risk Services ensure a BIA is conducted.

IS-12 Strategic Plan. Internal Audit recommends the Office of Information Technology update its IT recovery strategic plan to align with UC Merced's BIA and IS-12 requirements. The IT recovery strategic plan should address IT Recovery Plan development, training of the Unit IT Recovery Leads, the identification of a tool for developing and documenting IT Recovery Plans and developing processes to ensure units are held accountable for the development of their unit's plans.

Campus IT Recovery Plan. Internal Audit recommends OIT comprehensively update its Campus IT Recovery Plan. The plan should include an IT asset inventory and identification of IT recovery teams.

Cyber-risk Responsible Executive. Internal Audit recommends UC Merced appoint the CIO as the CRE.

IS-12 Exception Process. Internal Audit recommends OIT update the current IS-3 exception process to encompass IS-12 requirements.

BACKGROUND

UC Policy IS-12: IT Recovery

IS-12 was created as an acknowledgment by the UC for the need to protect its institutional resources and IT resources. As such, IS-12 provides a:

> systematic approach for planning the recovery of institutional information and IT resources managed by units, including units that have location-wide responsibility, such as central IT departments. This policy provides a framework for the governance, management, development, implementation, maintenance, and testing of an IT Recovery program.

Furthermore, locations are required to have a comprehensive emergency management program to comply with the UC Policy on Safeguards, Security, and Emergency. Per this policy:

> Each campus and the Office of the President will maintain a comprehensive and effective program encompassing risk assessment, risk mitigation, emergency preparedness and response, and business recovery to strengthen crisis and consequence management capabilities across the University system. The scope and composition of such programs will be based on an assessment of the most probable risks, hazards, and losses that may occur at a particular location.

A key aspect of the emergency management program is a Business Continuity Plan (BCP), which is one of the overarching processes for IT Recovery Planning.

Compliance with IS-12 – Iterative Approach

The UC recognizes the complexities of IT recovery planning and affords locations two methods of complying with policy requirements—the full compliance method and the iterative approach.

Through the full compliance methods, locations are expected to meet all the requirements of the policy. By adopting the iterative approach, locations are expected to use an iterative model that achieves the following:

- Assess an initial state of IT Recovery preparedness/readiness.
- Review and accept risks based on the Location BCP and BIA.
- Ensure that risk is accepted by a role with a level of authority corresponding to the level of risk.
- Include a review of regulatory compliance.

- Plan improvements to reach the target state, typically based on risk and resource availability.
- Implement improvements in IT Recovery to reach the target state.
- Assess the progress of policy implementation, IT Recovery Plans and implementation, and the state of IT Recovery readiness.
- Repeat the process as needed, with a minimum frequency of once per fiscal year.

UC Merced has adopted the iterative approach to compliance with IS-12 and OIT is working towards a risk-based, fiscally responsible level of compliance.

UC Ready

UC Ready is a web-based software tool used for continuity planning across the UC system. UC Ready supports continuity planning at the campus and department level, as well as IT disaster recovery planning efforts. The funding for UC Ready is provided by the UC Office of the President (UCOP).

SCOPE AND OBJECTIVES

This audit was selected based on a risk assessment and was performed as part of Internal Audit's responsibility to complete the fiscal year 2023 audit plan. The primary objective of the audit is to evaluate processes and controls in place to facilitate compliance with IS-12 requirements.

Additional objectives included:

- To assess the governance over IT recovery planning and processes.
- To evaluate the IT Recovery Plan controls exception process.
- To assess IT asset management process.
- To assess the sufficiency of the Location/Unit IT Recovery Plan.
- To assess the IT Recovery Plan testing process.

Internal Audit's primary scope included all of the OIT transactions and controls currently in place pertaining to IT recovery planning efforts. The audit included interviews of personnel, review of policies, observations and tests of current practices and processing techniques, and other auditing procedures considered necessary.

POSITIVE OBSERVATIONS

As stated in the University's mission, UC Merced strives for excellence in carrying out the university's mission of teaching, research, and public service. To achieve this mission, UC Merced stakeholders must be committed to the promotion of positive change in the university. As a result, Internal Audit is committed to highlighting practices in the areas audited that promote positive change within their organization and the university as a whole.

During the IS-12 Implementation audit, Internal Audit noted the following positive observations:

- OIT leadership has taken a thoughtful, risk-based approach to disaster recovery to ensure it is implemented in a fiscally efficient manner.
- OIT leadership currently is conducting risk assessments with units to better understand the IT risks of the campus departments.
- UC Merced has invested resources by hiring a business continuity planner to assist units in developing their BCPs.
- OIT and Risk Services have forged an effective, collaborative partnership.

OBSERVATIONS

1. BUSINESS IMPACT ANALYSIS

Background
IS-12 identifies the BCP and Business Impact Analysis (BIA) as the overarching controlling processes for the campus IT Recovery Plans and requires the campus IT Recovery efforts to align with BCP objectives. Per IS-12, the campus "uses its BCP and BIA to determine what business processes (Units) are in scope for IT Recovery planning."

A BIA is critical for the identification of the units on campus that are subject to IS-12 requirements. Furthermore, a BIA is beneficial in providing a sense of direction and effective use of resources for IT recovery planning.

Observation
During the preliminary survey meetings, Internal Audit noted UC Merced has not conducted a BIA. Per discussions with Risk Services staff, BIA efforts have been affected by budgetary and expertise constraints.

By not conducting a BIA, staff tasked with discharging IT recovery efforts could be ineffectively using limited resources. Furthermore, key areas could go unidentified and unprotected in the event of an IT disruption.

Recommendation
Internal Audit recommends Risk Services ensure a BIA is conducted.

Management Corrective Action
By January 1, 2024, Risk Services shall conduct a campus-wide business impact assessment focusing on Information Technology services and applications

2. IS-12 IMPLEMENTATION PLAN

Background
IS-12 requires Locations to devise IT recovery strategies that meet the needs of the Location. “Successful execution of an IT Recovery strategy requires commitment and planning involving Location senior management, the CRE, and Unit Heads”. These recovery strategies are risk based and use the BIA as the foundation for determining where resources should be invested. The strategic plan should include measurable milestones and deadlines to assess the efficiency of the plan and to ensure it is being achieved.

One of these measurable milestones includes the creation of IT Recovery plans for in-scope units. IS-12 requires in-scope units to develop a Unit IT Recovery Plan, which is “a formally documented, structured approach the describes how work can quickly resume after a disruption or disaster.” The plan must be developed in alignment with procedures outlined in section VI of IS-12. To maintain the relevance and effectiveness of the plans, Unit IT Recovery Leads must ensure these plans are updated and tested at least annually.

Internal Audit notes UC Merced utilizes UC Ready to create and centrally store unit business continuity plans (BCPs). UC Ready offers a BCP template that contains the level of detail required to comply with most IS-12 requirements.

Observation
The Office of Information Technology does not have a formalized and updated Implementation plan to comply with IS-12.

In addition, Internal Audit conducted a review of 12 BCPs and only one had IT recovery documentation; however, it did not align with IS-12 requirements.

Internal Audit notes UC Merced is still in the early stages of establishing a strategy for compliance with IS-12 and since there has not been a BIA conducted to identify the units that would need a Unit IT Recovery Plan, no Unit IT Recovery Plans have been fully developed.

Without a strategic plan and the foundational BIA, UC Merced cannot efficiently develop an effective IS-12 compliant IT Recovery Plan. Without an IT Recovery Plan, UC Merced has significant exposure to IT disruptions which could affect the financial and educational systems for the campus.

Recommendation
Internal Audit recommends the Office of Information Technology update its IT recovery strategic plan to align with UC Merced's BIA and IS-12 requirements. The IT recovery strategic plan should address IT Recovery Plan development, training of the Unit IT Recovery Leads, the identification of a tool for developing and documenting IT Recovery Plans, and developing processes to ensure units are held accountable for the development of their unit's plans.

Management Corrective Action
By April 30, 2024, OIT shall develop an IS-12 implementation plan that is responsive to the Business Impact Assessment (BIA)

3. CAMPUS IT RECOVERY PLAN

Background
Per IS-12, "IT Recovery Plans are fundamental to a location's ability to carry out its mission," and thus require campuses to develop a Campus IT Recovery Plan. This plan is informed by the BIA referenced in Observation 1 and is used to enable access to institutional information and enable business functions after an IT disruption.

The Campus IT Recovery plan should be approved by the cyber-risk responsible executive (CRE) and updated at least annually, ensuring campus IT recovery teams are identified and contact information is current, IT asset inventories are current, and recovery levels are appropriately assessed based on risk and needs of the business functions.

Observation
During the review of the IT Recovery Plan, Internal Audit noted UC Merced does not have an updated Campus IT Recovery Plan.

One major part of the campus IT Recovery Plan is an IT asset inventory, which is what management would use as the starting point for determining the recovery order of systems. During testing, Internal Audit noted that UC Merced does not have an IT asset

management process that fully aligns with IS-12 requirements. In addition, Internal Audit notes campus IT recovery teams have not been identified.

Per discussion with OIT staff, the plan has not been updated due to competing priorities in OIT. OIT has expended significant resources in becoming compliant with IS-3 and addressing cyber risk and IT issues as a result of the COVID-19 pandemic. Furthermore, UC Merced has not conducted a BIA which OIT acknowledges is required to inform and drive UC Merced's Campus IT Recovery Planning efforts.

Cyber risk insurance could be significantly higher or potentially unavailable if UC Merced does not have a valid Campus IT Recovery Plan. In addition, if a disaster happened without an actionable IT Recovery Plan, UC Merced could face unacceptable recovery times for essential IT systems.

Recommendation
Internal Audit recommends IT comprehensively update its Campus IT Recovery Plan. The plan should include the IT asset inventory and identification of IT recovery teams.

Management Corrective Action
By April 30, 2024, OIT shall collaborate with Risk Management services to update the campus recovery plan based on criticality of assets identified in the Business Impact Assessment

4. CYBER-RISK RESPONSIBLE EXECUTIVE

Background
IS-12 defines the cyber-risk responsible executive (CRE) as "an individual in a senior management role or academic position who reports to the Location chancellor or top executive. The CRE is accountable for all information risk assessments, security strategies, planning and budgeting, incident management, and information security implementation."

Per IS-12, the CRE is responsible for:

- Identifying a role (e.g., Location IT Recovery Lead, Risk Manager, Business Continuity Manager, or other suitable role) that will collect and share recovery team contact information with Units Location-wide.
- Approving:
    - The Location IT Recovery Plan.
    - The Location process of approving IT Recovery Plans.
    - The exception process.

  - Risk exceptions that impact the Location mission or IT Resources classified at RL4 and RL5.
  - Ensuring the testing frequency of IT Recovery Plans is adequate to address risk.
  - The storage location(s) for IT Recovery Plans.
  - The frequency of IT Recovery Plan testing.
  - The frequency of backup recovery testing.
- Participating in Location Recovery Plan testing once every three (3) years.
- Ensuring testing the frequency of the IT Recovery Plans adequately addresses mission risk related to BCP.
- Allocating funding to meet organization risk tolerances.
- Approving the governance process and managing the overall Location risk tolerance related to IT Recovery.
- Reviewing and approving significant gaps and risks requiring mitigations and evaluating associated mission risks with Location officers/Unit Heads.
- Reviewing with the Chancellor or Laboratory Director the state of Location readiness to perform IT Recovery.

Observation
During the preliminary survey meeting, Internal Audit noted the chief campus counsel is UC Merced's CRE. The chief campus counsel does not appear to have the necessary expertise and authority to discharge key roles and responsibilities as the campus' CRE. Internal Audit notes the chief information officer (CIO) is currently performing most of the CRE responsibilities.

Per discussions with OIT staff, when the new version of the IS-12 rolled out, campuses were given general guidance on who can be appointed as the CRE. As a result, locations appointed CREs that ranged in titles. UC Merced decided to appoint the chief campus counsel as the CRE because, at the time, the CIO role reported to the provost and, therefore, did not qualify to be the CRE.

Recommendation
Internal Audit recommends UC Merced appoint the CIO as the CRE.

Management Corrective Action
Internal Audit notes that during the course of the audit, UC Merced appointed the CIO as the CRE thus no additional Management Corrective Action is required.

5. IS-12 EXCEPTION PROCESS

Background
The University of California acknowledges the need for campuses to periodically deviate from the IS-12 policy and therefore requires campuses to have an approved exception process. IS-12 requires the approved campus exception process to include the following:

- Exception process approval
- Exception circumstances
- Documentation
- Unit requirements
- Exception approvals

Observation
OIT does not have an exception process that is in scope of IS-12 requirements. However, Internal Audit notes OIT has an exception process For UC Policy IS-3: Electronic Information Security that lends itself to be modified to include IS-12 requirements.

Recommendation
Internal Audit recommends OIT update the current IS-3 exception process to encompass IS-12 requirements.

Management Corrective Action

By November 30, 2023, OIT shall incorporate IS-12 into the IS-3 exception process