Internal Audit Report

IT Recovery / Business Continuity

Report No. SC-23-05
March 2023

Steve Architzel
Auditor in Charge

Approved
James Dougherty, Director
Audit & Management Advisory Services
Table of Contents

I. EXECUTIVE SUMMARY.................................................................................................................................. 2

II. INTRODUCTION
Purpose.......................................................................................................................................................... 3
Background.................................................................................................................................................... 3
Scope ............................................................................................................................................................. 4

III. Results ........................................................................................................................................................... 5
I. EXECUTIVE SUMMARY

Audit & Management Advisory Services completed a review of the implementation of IS-12 IT Recovery Policy. This audit was included on our FY23 Audit Plan.

During initial meetings with ITS leadership, it was readily acknowledged that UC Santa Cruz had not yet implemented IS-12. Therefore, the purpose of this audit was modified from seeking to determine if the policy has been implemented, to instead determining what sort of barriers may exist in implementing the policy. The IS-12 policy does acknowledges that units have limited IT budgets and consequently the policy allows for an iterative, risk-based, approach for the units to make improvements over time/budget cycles.

A. ITS has created internal working documents that define tangible and measurable steps to move into compliance with IS-12 over time and also makes note of resource requirements for these actions. However, ITS should formalize these steps, include tangible deliverables with due dates, and obtain ITS senior leadership endorsement on the roadmap.

One Key requirement of IS-12, is for units to create IT Recovery Plans. While ultimately this responsibility lies with unit heads, ITS could play an important facilitation role in enabling units to more easily develop, maintain, and refine these plans in line with the policy’s iterative approach. During our review, we found that it was unlikely that many units have presently completed these plans. However, at the time of the audit, ITS was currently drafting an IS-12 IT Recovery Program Plan to move into compliance with this requirement, and we were provided a work-in-progress version of it. The elements required of an iterative method were included in the ITS plan. Therefore, units could get into compliance with the policy by modeling from an ITS plan.

B. A Key requirement of IS-12, is for units to create IT Recovery Plans. While ultimately this responsibility lies with unit heads, ITS could play an important facilitation role in enabling units to more easily develop, maintain, and refine these plans.

Finally, in an effort to determine what potential barriers may exist with the implementation of IS-12 at the unit level, we sent a survey to these individuals likely to be in these roles. Of the approximately 150 surveys sent out, we received 36 responses which are reported near the end of this report.

More details are in the body of the report.
II. INTRODUCTION

Purpose
The purpose of this review is to examine the preparation for the implementation of IS-12 IT Recovery Policy to ensure that the campus is ready for the full implementation of this policy. This audit was included on our FY23 Audit Plan.

Our scope was focused on activities that the campus should have worked on in preparation for the full implementation of IS-12. This specifically includes reviewing:
• Use local governance and the location’s business continuity plan.
• Identification of key personnel.
• The basic recovery plan.
• The processes for approving IT recovery plans and granting exceptions.

Background
UC policy, IS-12, is intended to guide and prepare for IT recovery and business continuity in the event of an unavoidable or unforeseen disaster. The IT Recovery requirements in IS-12 provide 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. The policy provides a framework for the governance, management, development, implementation, maintenance, and testing of an IT recovery program.

While ITS should play a key role in facilitating the implementation of the policy, ultimately much of the implementation of IS-12 will need to occur at the unit level. IS-12 includes a number of roles and responsibilities for implementing the policy:
• The location’s cyber-risk responsible executive is a senior executive appointed under the IS-3 Electronic Information Security Policy, has broad authority and responsibility to oversee the implementation of this policy.
• The policy uses the term unit head to refer to a dean, vice chancellor or person in a similarly senior role who has the authority to allocate budget and is responsible for unit performance and administration.
• Unit IT recovery leads are individuals appointed by unit heads that play a key role in overseeing the unit’s IT Recovery Plans. In practice, at UC Santa Cruz many individuals who are unit information security leads (UISL), as defined in IS-3, will likely also be involved in taking on unit IT recovery lead roles defined in IS-12.
• A workforce member refers to an employee, faculty, staff, volunteer, contractor, researcher, student worker, student supporting/performing research, medical center staff/personnel, clinician, student intern, student volunteer, or person working for UC in any capacity or other augmentation to UC staffing levels.

The policy was updated on July 1st, 2021 from a 2007 version and it specifies that locations must transition planning and execution from the prior version to the current version 12 months after the update. Therefore, locations should have transitioned by July 1st 2022. However, the policy also notes that given limited unit IT budgets, unit heads may experience gaps in their IT recovery solution. In these cases, cyber risk executives and unit heads must use an iterative risk-based approach, making
improvements over time/budget cycles, and ensuring that location executives understand the remaining risks.

Scope

The scope of this review included:

- Interviewing key individuals from ITS and the Office of Emergency Management,
- Reviewing UCOP policies on IS-12,
- Reviewed various local planning documents related IS-12 implementation and business continuity
- Surveyed approximately 150 current UISLs, which will likely also play a role as unit IT recovery leads to determine what barriers may exist in implementing IS-12.
III. Results

During initial meetings with ITS leadership, it was readily acknowledged that UC Santa Cruz had not yet implemented IS-12. Therefore the purpose of this audit was modified from seeking to determine if the policy has been implemented, to instead determining what sort of barriers may exist in implementing the policy.

A. Development of IS-12 Implementation Roadmap

ITS has created internal working documents that define tangible and measurable steps to move into compliance with IS-12 over time and also makes note of resource requirements for these actions. However, ITS should formalize these steps, include tangible deliverables with due dates, and obtain ITS senior leadership endorsement on the roadmap.

Risk Statement/Effect

Without target dates with tangible deliverables, it will be difficult to determine what progress is being made, and/or if any course correction is needed, towards implementing IS-12.

Agreement

| A1 | The Vice Chancellor, ITS, should create and approve a formal “roadmap” for the campus implementation of IS-12 to include determining target implementation dates for deliverables needed to facilitate the implementation of IS-12 as well as noting any resource requirements/constraints related to these deliverables. | Implementation Date
| | | September 30, 2023 |
| | | Responsible Manager
| | | Vice Chancellor, ITS |
| | | Aisha Jackson |

A. Development of IS-12 Implementation Roadmap

As mentioned in the background section, the IS-12 policy does acknowledges that units have limited IT budgets and consequently the policy allows for an iterative, risk-based, approach for the units to make improvements over time/budget cycles. Section 1.3.2 of the IS-12 policy provides specific requirements for using an Iterative method:

- Assess an initial state of IT recovery preparedness/readiness.
- Review and accept risks based on the location Business Continuity Plan.
- 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.
During our review, we found that it is unlikely that many units have presently completed all of these requirements for using this iterative approach. At the time of the audit, ITS was currently drafting an IS-12 IT Recovery Program Plan for its division to move into compliance with this requirement, and we were provided a work-in-progress version of it. The elements required of an iterative approach were laid out in the ITS plan. Therefore, units could get into compliance with the policy by following the plan ITS laid out.

We observed five overall objectives of the working documents ITS was in the process of developing at the time of our review:

- Develop a robust, enterprise-level IT Recovery Program.
- Comply with IT Recovery (IS-12) policy.
- Perform an initial assessment of IT Recovery preparedness/readiness.
- Create IT Recovery Plans for UCSC and Units.
- Assess progress of policy implementation, IT Recovery plans and the state of IT Recovery preparedness/readiness

For each of these five overall objectives, the plan further broke them down into smaller, tangible deliverables. This is a good practice. Additionally, there was space to include target implementation dates for these deliverables, but at the time of our review no target dates were included. Without target dates, it would be difficult to determine what progress is being made, and/or if any course correction is needed towards implementing IS-12.

While target dates may be contingent on resource constraints, it is nevertheless important to have some targets in order to provide some way to measure progress towards implementation of the policy over time. Therefore, ITS should determine target implementation dates for deliverables needed to facilitate the implementation of IS-12.

### B. Development of Unit IT Recovery Plans

<table>
<thead>
<tr>
<th>Agreement</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>B.1</td>
<td>The associate vice chancellor, Information Security, should provide guidance to unit heads on how to locally develop and implement IT Recovery Plans. This guidance could take the form of:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• In person or remote training sessions,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Example IT recovery plan templates within UC Ready,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Providing initial assessments of unit’s IT readiness,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation Date</td>
<td>September 30, 2023</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsible Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Associate Vice Chancellor, Information Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brian Hall</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
B. Development of Unit IT Recovery Plans

A natural way for units to create and store their recovery plans would be by using UC Ready, and indeed this appears to be the approach endorsed by ITS. UC Ready is a system-wide, web-based software tool built on the Salesforce platform for business continuity planning. While the software was initially used at UC for business continuity planning, it has grown to include IT Disaster Recovery. ITS could, and should, provide guidance to units on how to create IT Recovery Plans and use the UC Ready software.

Work-in-progress planning documents I reviewed from ITS included deliverables providing guidance to units such as with:
- In person or remote training sessions,
- Example IT recovery plan templates within UC Ready,
- Providing initial assessments of unit’s IT readiness,
- Etc.

This sort of guidance from ITS would be beneficial for facilitating units’ implementation of IS-12. While, these elements appeared in work-in-progress, it is important that the planning work is finalized. Therefore, ITS should finalize this planning effort in progress and ensure it has buy-in from ITS leadership.

C. Observations and Results of Survey

The auditor made a few observations that leaders should be aware of in planning for IS-12 Implementation:
- In practice, the folks units will most likely use to fill the role of IT recovery leads, are already filling the roles of Unit Information Security Leads required under IS-3.
- Both the roles of IT recovery leads and Unit Information Security Leads are typically tasked as additional duties for individuals within divisions rather than someone’s fulltime job. Therefore these folks who are already burdened by the additional duties of Unit Information Security Leads will be asked to do even more under IS-12.
- Perhaps the most common comment that came up in the survey results was in regards to the limited amount of time folks have to dedicate to the rolls of IT recovery given their other rolls.
- In reviewing the survey results, it appears that smaller units tend to have larger IT knowledge related problems. This is somewhat logical as smaller units would have fewer individuals to draw on to perform the rolls of IT recovery leads. Therefore special attention may need to be given to some of these smaller units in regards to training.

As previously mentioned, while ITS plays a key role in facilitating the implementation of IS-12, ultimately much of the work will need to be done at the unit level by the unit heads and the unit IT recovery leads.
In order to determine what potential barriers may exist with the implementation of IS-12 at the unit level, we sent a survey to the individuals likely to be in these roles. Of the approximately 150 surveys sent out, I received 36 responses:

<table>
<thead>
<tr>
<th>What is your affiliation(s) to UC Santa Cruz Information Security?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit Head and Unit Information Security Lead</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>Unit Information Security Lead</td>
</tr>
<tr>
<td>30</td>
</tr>
</tbody>
</table>

The results of the survey are as follows.

---

1 We could not determine if there is currently a list of individuals in the IT recovery lead roles. However, we were able to get a list of individuals currently appointed as unit information security leads. It is likely that there will be overlap of individuals appointed to both roles and therefore we are confident that the results are relevant.
**ARE YOU FAMILIAR WITH THE RESPONSIBILITIES FOR THE FOLLOWING ROLES UNDER IS-12?**

<table>
<thead>
<tr>
<th>Role</th>
<th>Very Familiar</th>
<th>Very Good Understanding</th>
<th>General Understanding</th>
<th>Limited Understanding</th>
<th>Not Familiar</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Manager</td>
<td>16</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Business Continuity Planner</td>
<td>15</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Cyber Risk Executive</td>
<td>20</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Unit IT Recovery Leads</td>
<td>11</td>
<td>7</td>
<td>6</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Unit IT Recovery Teams</td>
<td>13</td>
<td>8</td>
<td>7</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Unit Head</td>
<td>12</td>
<td>8</td>
<td>7</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Unit Information Security Lead</td>
<td>9</td>
<td>9</td>
<td>4</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Workforce Member</td>
<td>12</td>
<td>9</td>
<td>6</td>
<td>4</td>
<td>7</td>
</tr>
</tbody>
</table>

Do you see any barriers to identifying assets covered by IS-12?

- 1. Very Difficult to identify applicable assets: 29%
- 2: 8%
- 3: 14%
- 4: 26%
- 5. Relatively easy to identify applicable assets: 23%
Are you familiar with "Business Continuity Planning?"

- Yes. I am quite familiar with Business Continuity Planning.
- Generally Yes. I have a good understanding of Business Continuity Planning.
- Moderate. I have a general understanding of Business Continuity Planning.
- Generally No. I am aware of Business Continuity Planning, but I have little knowledge of what it entails.
- No - I haven’t heard of Business Continuity Planning.

Do you see significant barriers in ensuring IT continuity is aligned with your unit's business continuity planning efforts?

- I am not aware of any barriers in Ensuring Alignment between IT and Business Continuity: 10
- Time/Resources Constraints (few resources allocated to these efforts): 13
- The Unit does not have an effective Business Continuity Plan Currently in Place or that Plan is Unclear: 7
- Knowledge Constraints (little expertise within the Unit regarding Business or IT Continuity): 7
- Organizational Limitations (Roles within the Unit are not well suited to ensure Continuity Efforts are Successful): 5
- N/A - I am not familiar Enough with Business Continuity Planning within my Unit to Address this Question: 8
- Other: 1
Has your unit recently performed any sort of IT recovery testing?

- 1 - No - I'm not aware of any.
- 2
- 3
- 4
- 5 - Yes - My unit regularly does IT recovery testing.

Do you see any significant barriers in performing IT recovery testing?

- We don't have sufficient policy/guidance in place to guide this testing.
- Knowledge constraints (little expertise within the unit to perform these tests).
- Time/resources constraints (few resources allocated to these efforts).
- Organizational limitations (roles within the unit are not well suited to perform these tasks).
- I am not aware of any barriers.
- N/A - I am not familiar enough with this topic.