UNIVERSITY
OF
CALIFORNIA

**IS-12 IT Recovery
FAQ
security.ucop.edu**

Frequently Asked Questions

General questions

1. Is there a guide to help non-specialists understand UC-specific and technical terms in IS-12?

Yes. All definitions are included in the IT Policy Glossary. IS-12 terms align with those of IS-3. Training materials also include explanations for non-specialists. See: https://security.ucop.edu/files/documents/policies/it-policy-glossary.pdf

2. How does IS-12 treat cloud technology specifically?

The revision includes cloud-friendly language. It also features cloud specific supplier requirements, ranging from choosing a capable supplier to recovering from disasters that impact suppliers.

3. How are faculty involved in the IT recovery process?

Faculty play a significant role in the IT recovery process. The Research Data Security Workgroup has focused on this priority and published a report, available here https://security.ucop.edu/resources/location-data-security.html. IS-12 training and support materials will also address faculty involvement. The scope of involvement will be set by each Location based on Business Impact Analysis (BIA) and emergency management based recovery priorities.

4. How can UC community members learn more about Recovery Time Objectives (RTOs)?

This is a key concept for business continuity planning. It will be a focus of the training and roll-out. This is explicitly addressed in the training and online resources.

5. How does IS-12 distinguish between IT recovery teams? What is the difference between the Location IT Recovery Team, and Unit IT Recovery Team?

The Location Recovery Team focuses on core IT services. These typically included services like networking, telecom, email, directory, authentication, and other services that impact the Location at large. Unit IT Recovery Teams typically focus on specific business processes. Unit business processes that might be in scope include student health services, financial aid, fire safety systems, and building access systems.

6. Do Recovery Levels conflate the cost of downtime with the cost of permanent loss?

No. Recovery Levels (designated as R1-R5) focus only on the speed of recovery to support the Location business continuity plan (BCP). Tiering of assets is a fundamental core concept of IT Recovery planning, testing and communication. These common Recovery Time Objectives (RTO) are the basis for investment and technical decisions.

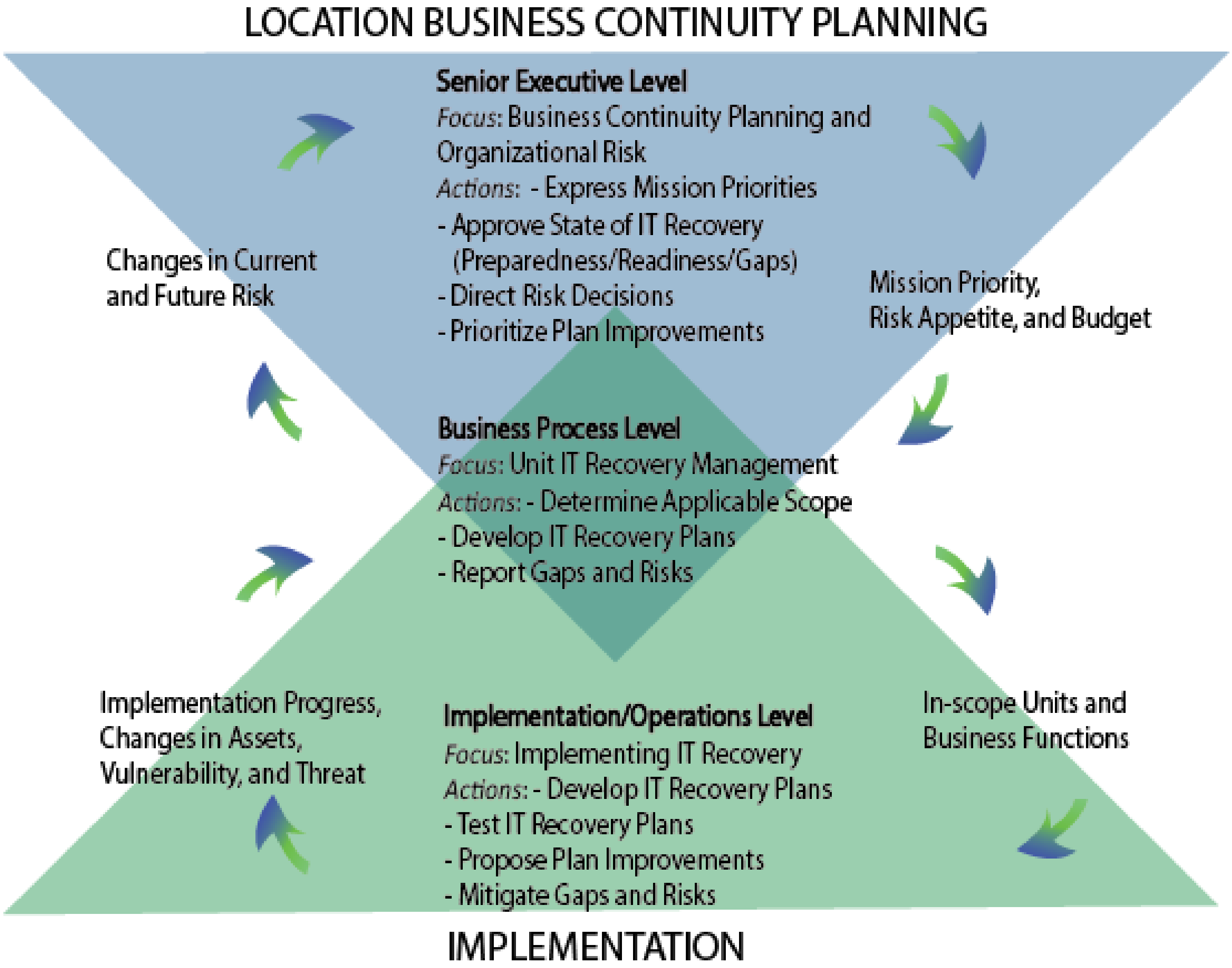
Very valuable data can have a low Recovery Level. That same data may have a high Availability Level (AL) under IS-3 Electronic Information Security. When the Availability Level is high, additional controls are in place to manage risks related to the loss of availability. The assigned Recovery Level is only concerned with the speed of bringing the service or asset back into use based on the Location BCP.

7. Are there specific requirements related to research data under IS-12?

No. However, the new IS-12 lets each Location set specific requirements based on their needs, which means that certain programs, technology, or capability may be included in the IT Recovery Plan, including specific research programs or instructional technology.

8. How can Locations better plan for an iterative process of compliance?

IS-12 calls for Locations to “allocate resources to protect Institutional Information and IT Resources based on their value, risk factors, likelihood, and severity of the impact of potential events causing an adverse outcome.” Requirements for the iterative process are based in NIST-CSF. Please refer to this diagram outlining the UC process, which is adapted from NIST for UC.


LOCATION BUSINESS CONTINUITY PLANNING
Senior Executive Level
Focus: Business Continuity Planning and Organizational Risk
Actions: - Express Mission Priorities
- Approve State of IT Recovery (Preparedness/Readiness/Gaps)
- Direct Risk Decisions
- Prioritize Plan Improvements
Changes in Current and Future Risk
Mission Priority, Risk Appetite, and Budget
Business Process Level
Focus: Unit IT Recovery Management
Actions: - Determine Applicable Scope
- Develop IT Recovery Plans
- Report Gaps and Risks
Implementation Progress, Changes in Assets, Vulnerability, and Threat
In-scope Units and Business Functions
Implementation/Operations Level
Focus: Implementing IT Recovery
Actions: - Develop IT Recovery Plans
- Test IT Recovery Plans
- Propose Plan Improvements
- Mitigate Gaps and Risks
IMPLEMENTATION

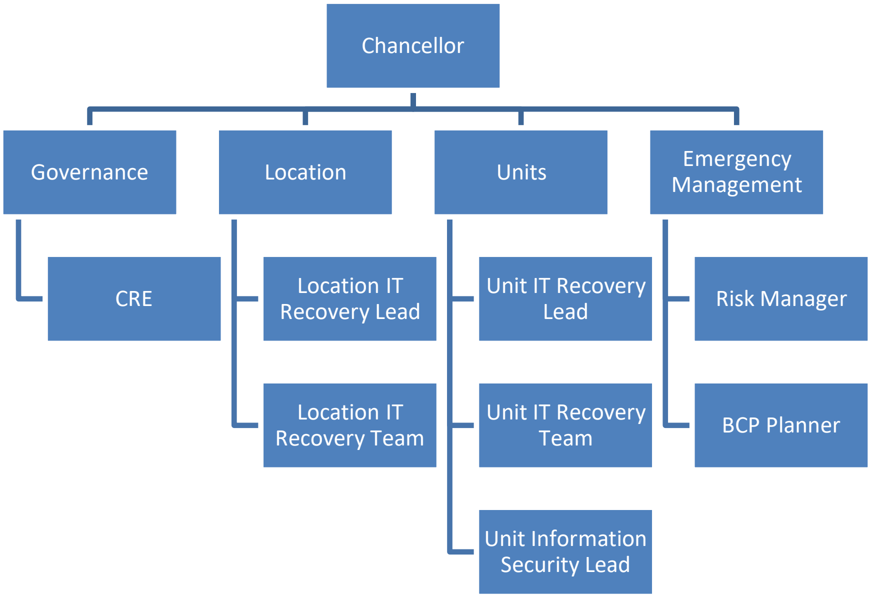
9. Does the IS-12 require new roles and therefore new budgetary requirements?

No. The IS-12 rewrite assigned new names to already designated roles in order to align with IS-3 terminology.

For example, the VP Business Ops is now the Cyber-risk Responsible Executive (CRE); the Department Head is now the Unit Head; and Assigned Individuals is now the IT Recovery Lead (ITRL).

10. Is there an organization chart to help community members understand processes and duties?

Yes. The chart below represents the process logic reflected in IS-12 (not reporting relationships).



Note: Locations may use the term Emergency Management or Organizational Resiliency.

11. Is the term "designee" a formal delegation of authority?

No. In the roles and responsibilities table in IS-12, the Unit Head role can delegate two tasks or responsibilities under the policy. This is not the same as the Regental Delegation of Authority. This use of the term "delegation" follows the word's common meaning, which is that the assigned role can task another to implement or carry out the duties.

12. Does the Chancellor approve the Location IT Recovery Plan?

No. In IV.1.1.5, the requirement is that "CREs must review with the Chancellor or Laboratory Director the state of Location readiness to perform IT Recovery at least once every two (2) years." This review could expose risks or gaps that the Chancellor might choose to have the CRE reduce or eliminate. The requirement is to ensure Chancellors have visibility, but approval rests with the CRE. This is consistent with CRE appointment requirements.

The review meeting should be documented consistent with Location best practices.