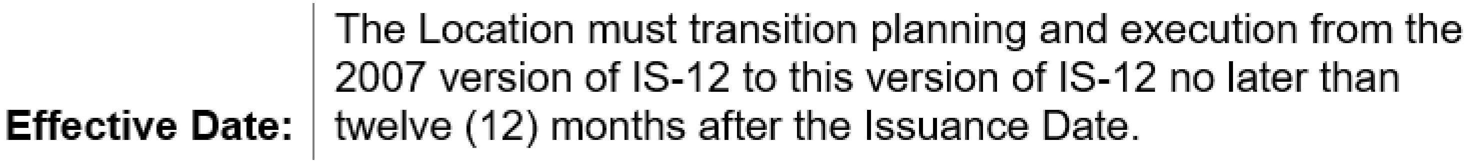
IS-12 IT Recovery Policy Key Features

SUMMARY

ROBERT SMITH

ROBERT.SMITH@UCOP.EDU

Effective Date

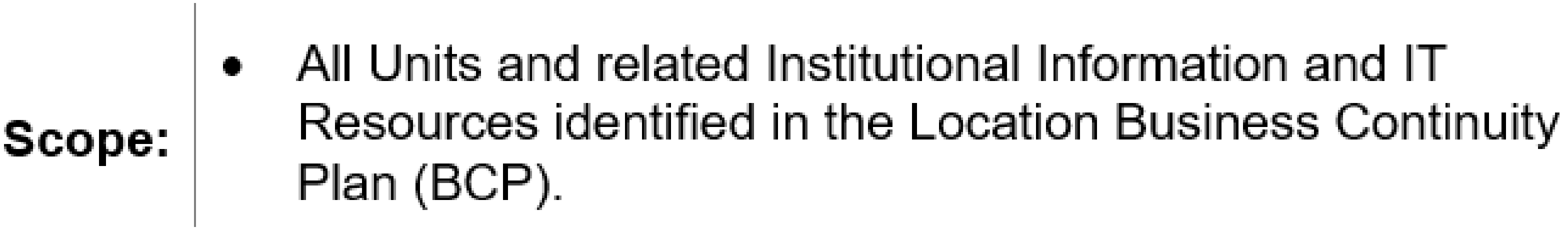


Effective Date: The Location must transition planning and execution from the 2007 version of IS-12 to this version of IS-12 no later than twelve (12) months after the Issuance Date.

12 Months to move to the new iterative model!

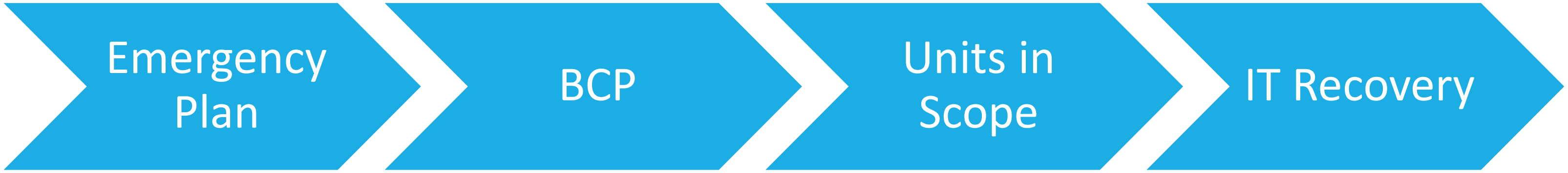
Resets the compliance clock!

Limited scope based on Location BCP



Scope:

- All Units and related Institutional Information and IT Resources identified in the Location Business Continuity Plan (BCP).



Emergency Plan

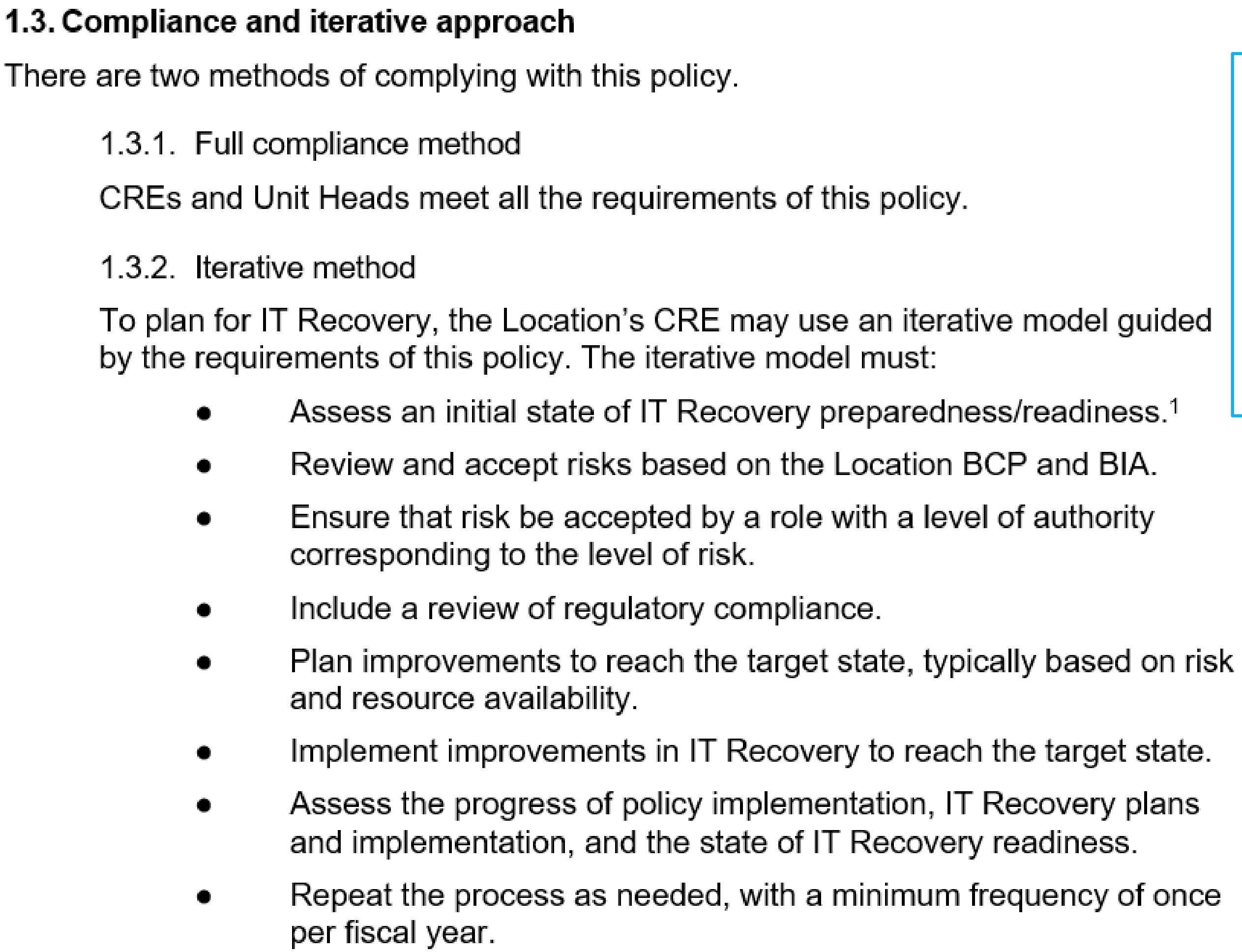
BCP

Units in Scope

IT Recovery

Location planning and priorities now drive scope and implementation.

New iterative model – based on IS-3/CSF



1.3. Compliance and iterative approach

There are two methods of complying with this policy.

1.3.1. Full compliance method

CREs and Unit Heads meet all the requirements of this policy.

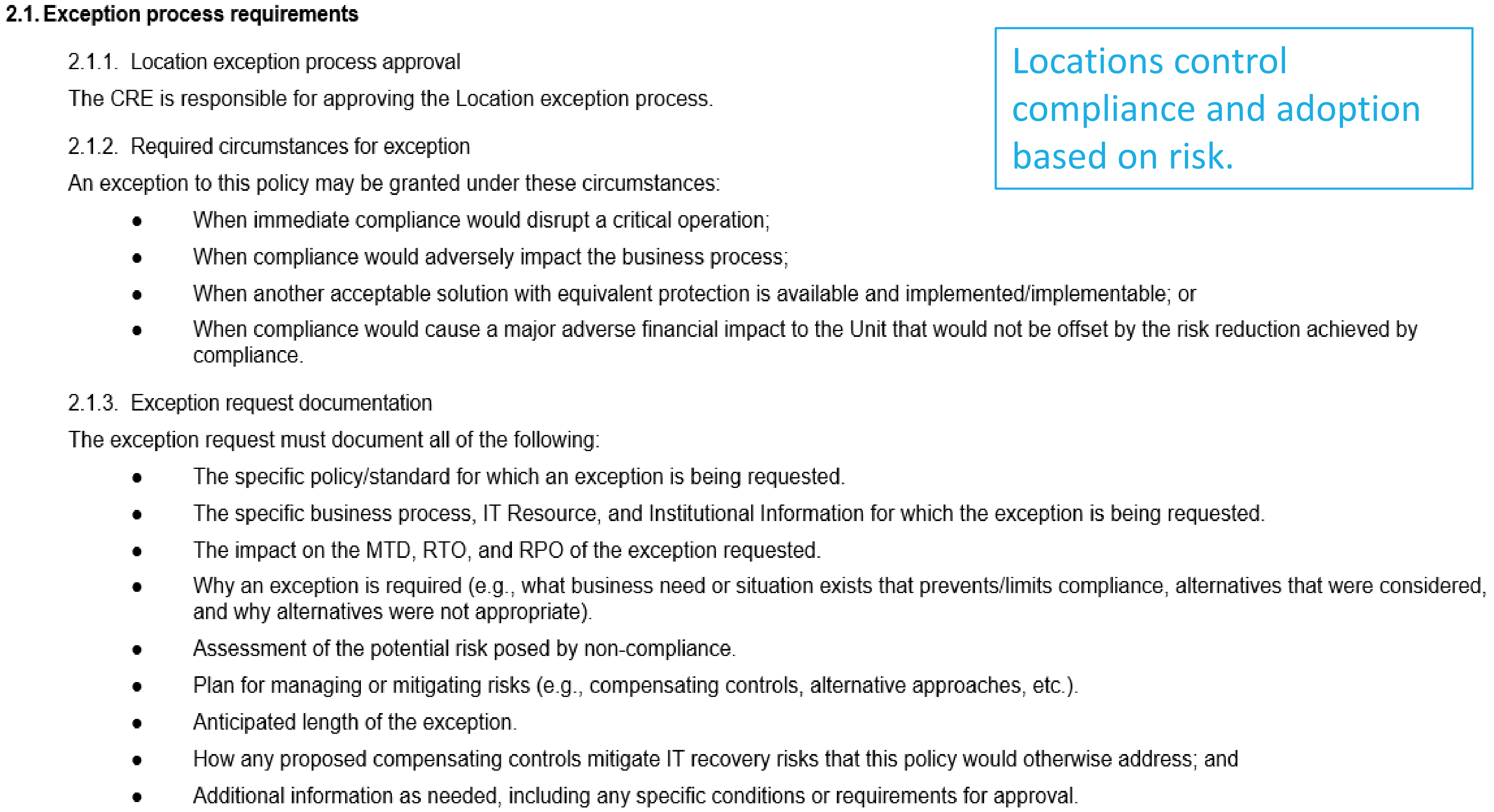
1.3.2. Iterative method

To plan for IT Recovery, the Location's CRE may use an iterative model guided by the requirements of this policy. The iterative model must:

- Assess an initial state of IT Recovery preparedness/readiness.[1]
- Review and accept risks based on the Location BCP and BIA.
- Ensure that risk be 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.

These methods allow the Location to iterate over years to fully address IT Recovery risk and manage to a desired level.

Robust Location Exception Process



2.1. Exception process requirements

2.1.1. Location exception process approval

The CRE is responsible for approving the Location exception process.

2.1.2. Required circumstances for exception

An exception to this policy may be granted under these circumstances:

- When immediate compliance would disrupt a critical operation;
- When compliance would adversely impact the business process;
- When another acceptable solution with equivalent protection is available and implemented/implementable; or
- When compliance would cause a major adverse financial impact to the Unit that would not be offset by the risk reduction achieved by compliance.

2.1.3. Exception request documentation

The exception request must document all of the following:

- The specific policy/standard for which an exception is being requested.
- The specific business process, IT Resource, and Institutional Information for which the exception is being requested.
- The impact on the MTD, RTO, and RPO of the exception requested.
- Why an exception is required (e.g., what business need or situation exists that prevents/limits compliance, alternatives that were considered, and why alternatives were not appropriate).
- Assessment of the potential risk posed by non-compliance.
- Plan for managing or mitigating risks (e.g., compensating controls, alternative approaches, etc.).
- Anticipated length of the exception.
- How any proposed compensating controls mitigate IT recovery risks that this policy would otherwise address; and
- Additional information as needed, including any specific conditions or requirements for approval.

Locations control compliance and adoption based on risk.

Noteworthy Comparison

Improvements addressed

- Added new features
  - Narrower scope – Location defined.
  - Exception process.
  - Iterative model for compliance.
- Clock restarts – 12 months to transition.
- The current policy does not align with UC Health recovery levels. Aligning helps UC Health and:
  - UCLA
  - UC Davis
  - UCI
  - UCSD

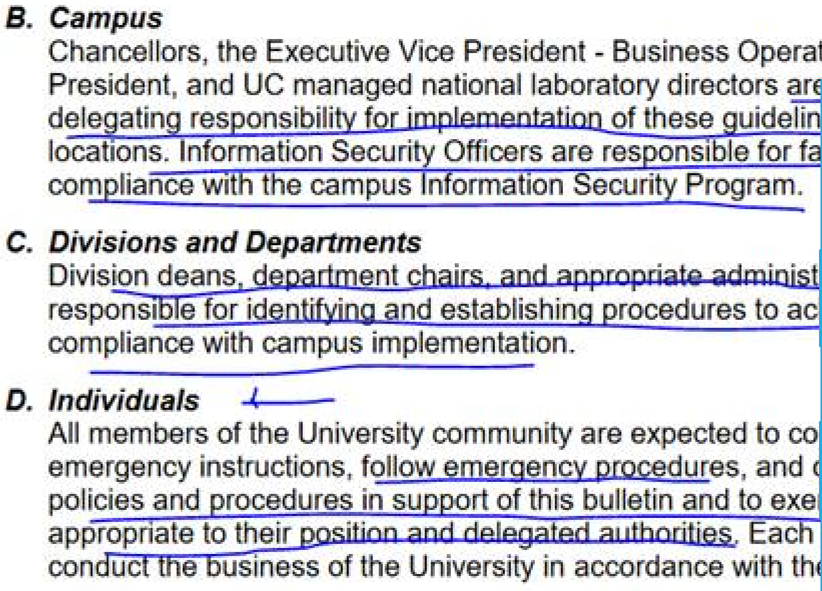
Advantages of the Rewritten Policy

- Now aligned with technology.
- Aligns with UC Health Recovery levels.
- Now aligned with Cloud and Service Providers.
- Directly implementable.
- Systemwide consistency.
- Endorsed by systemwide workgroup, including BCP leads

Sponsored by:

- UCACC/AS
- Risk Services
- Systemwide IT

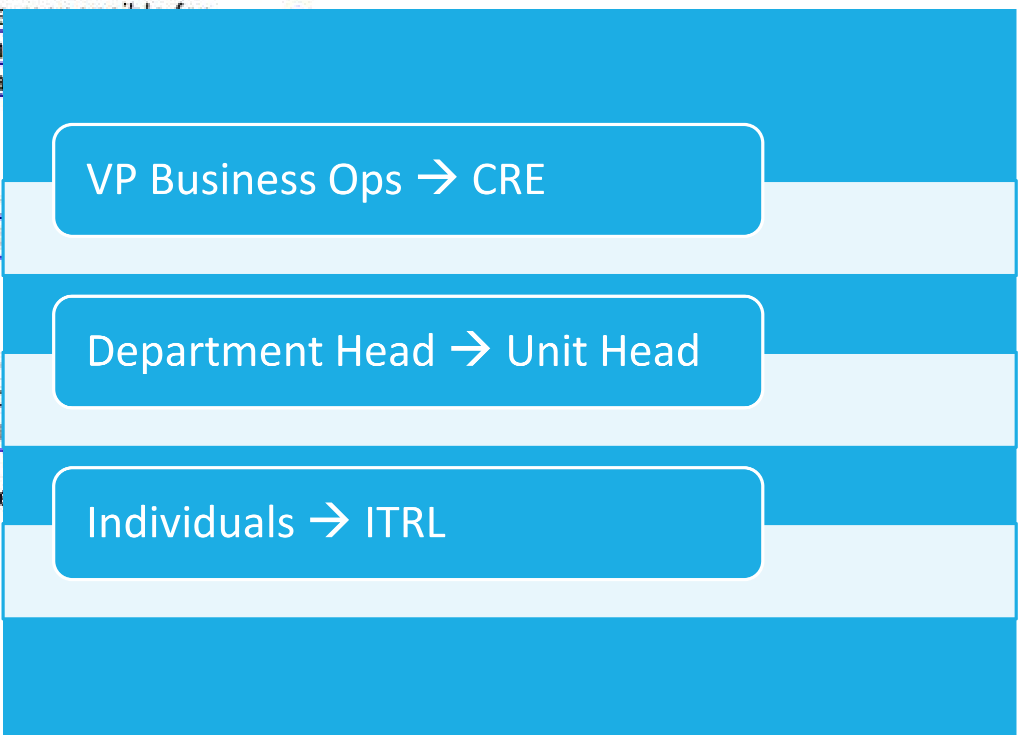
Old IS-12 Roles map to new!



B. *Campus*
Chancellors, the Executive Vice President - Business Operations at the Office of the President, and UC managed national laboratory directors are delegating responsibility for implementation of these guidelin locations. Information Security Officers are responsible for fa compliance with the campus Information Security Program.

C. *Divisions and Departments*
Division deans, department chairs, and appropriate administ responsible for identifying and establishing procedures to ac compliance with campus implementation.

D. *Individuals*
All members of the University community are expected to co emergency instructions, follow emergency procedures, and policies and procedures in support of this bulletin and to exe appropriate to their position and delegated authorities. Each conduct the business of the University in accordance with the



VP Business Ops → CRE

Department Head → Unit Head

Individuals → ITRL

Old blocks mapped to new

Current IS-12	New IS-12
	Identify – roles/people
Mitigation	Removed from IS-12 – this topic is covered in IS-3 IR Standard
Technology and Infrastructure	Same
Preparedness	Same + communication plan
Response	Same
Recovery	Same

thank you!

QUESTIONS – CONTACT: robert.smith@ucop.edu