

Contingency Planning Guide Review

General comments:

As already mentioned, this needs to be more than a shortened NIST 800-34. This comes out in two ways:

- Because NIST Special Publications provide recommendations to how agencies should implement IT security, the language used in their documents reflects that point of view. Departmental guidance, on the other hand, should mandate how the department *will*, not *should*, conduct its business. Soft language ("should", "recommend", etc.) should be replaced with directions ("must", "required", "will" etc.). In one paragraph on training (3.6.2, first paragraph), five "should"s are used in a four sentence paragraph. I doubt that the Department will later agree that no one is required to follow any of this guidance because the language implies it's all optional.
- The document still does not describe its terminology and requirements consistently. Calling a Continuity of Support and an IT Contingency Plan the same thing, and then saying the whole process is called IT Contingency Planning is confusing (footnote, p.1). More confusing however, is requiring a DRP and COS for the IT Contingency Planning process, and then stating that many COS plans include DRPs without giving clear guidance when this is the case. We recommend reviewing the document with consistency and clarity in mind. People not intimately familiar with the terminology will need to implement this guide. Make their lives easier.

Specific comments:

Footnote 1, p.1; Sect 2.5.1, p.7; Table 2-2, p.7 Inconsistent use of Continuity of Support vs. IT Contingency Plans.

Recommendation/comment: Stick with the definition provided in the first footnote.

Sect 2.3, p.4 "During the contingency planning phase, recovery procedures are identified and incorporated into the plan to ensure the availability of GSSs or MAs in the event of a natural or man-made disaster."

Recommendation/comment: Instead of "natural or man-made disaster", use "natural or man-made disruption" so as to include COS situations.

Sect 2.3, p.4 "During the contingency planning phase, recovery procedures are identified ..."

Recommendation/comment: What contingency planning phase? Phase of what? There isn't a contingency planning phase of C&A or the SDLC.

Sect 2.3, p.4 "For example, a system requiring encryption, intrusion detection or virus protection under normal operations should ensure that operations in recovery mode are also operating on encrypted systems."

Recommendation/comment: This sentence provides an example of a system requiring encryption, IDS and virus protection, but then only refers to encryption in its solution. Generalize the ending using "with equivalent protection".

Sect 2.4, p.4 List of subteams.

Recommendation/comment: Add GSS/MA Coordination to the list of teams.

Sect 2.4.1, p.4 "It is recommended that a senior management official, such as the Principal Officer, serve as the head of the Management Team."

Recommendation/comment: Why recommend someone as high as the PO be the lead of the Management team? In a COS situation especially, that seems somewhat extreme. Shouldn't the System Manager have that responsibility instead?

Sect 2.5, p.5

Recommendation/comment: Delete "IT Contingency Plan" from the paragraph and table, as per the footnote on p.1. Also, spell out DRP.

Sect 2.5.1, p.6

Recommendation/comment: Delete "IT Contingency Plan" from the paragraph and title.

Sect 3.2.2, p.8 "...the appropriate amount of time should be spent to adequately document the results."

Recommendation/comment: This is an extraordinarily vague comment for a guidance document.

Sect 3.2.3, p.9

Recommendation/comment: Add a reminder that in the case of a widespread catastrophe, ED system recovery will be a lower priority than health, safety or military systems operated at shared recovery facilities.

Sect 3.3, p.10 Last paragraph - "All preventive measures in place should be maintained periodically to ensure their effectiveness."

Recommendation/comment: Should instead be "maintained and tested periodically".

Sect 3.4.1.3, p.11 Geographic proximity

Recommendation/comment: Mention that excessive distance may lengthen recovery times.

Sect 3.4.1.3, p.12 "At no time, should a staff member's home be considered for off-site storage."

Recommendation/comment: Has it been a big problem at the department of people storing backups at their house?

Sect 3.4.2, p.12 Alternate site options

Recommendation/comment: After the three options, again remind readers that if choosing the latter two options, their systems may receive lower priority if they share facilities/resources with health, safety or military systems.

Sect 3.4.2, p.13 Mobile Sites

Recommendation/comment: Although good for thoroughness, it is extremely doubtful that ED systems would ever use a mobile backup site.

Sect 3.4.4, p.15 "Subteams may include staff with these areas of expertise:"

Recommendation/comment: Is the list provided a list of desired expertise, or a repeat of section 2.4's subteams? If the former, better descriptions of actual expertise should be used.

Sect 3.6, p.16 Plan Testing, Training, and Exercising

Recommendation/comment: What are the requirements of COS testing vs. DRP testing?

Sect 3.6.1, p.17 Plan Training and Exercises

Recommendation/comment: How specifically should plans be tested (examples, recommendations, etc.)?

Sect 3.7, p.18 "As deficiencies in the plan are identified through testing and through exercises, the system manager should identify and implement corrective measures and provide updates to appropriate Department personnel, as defined in the Department's *IT Security Policy*, *OCIO Security Policy Guidance*, and the *IT Security Compliance Plan*."

Recommendation/comment: What does the IT Security Compliance Plan have to do with maintaining a contingency plan?

Sect 3.7.1, p.18; Sect 3.7.2, p.19 Plan version control/supporting documentation

Recommendation/comment: Discuss how to coordinate the distribution of changes to the plan and supporting documentation.

Sect 4.2.3, p.24 Plan Activation

Recommendation/comment: Discuss what should occur in the event that the CPC is unavailable, as well as if the CPC's alternate is also gone.

Sect 4.3.2, p.25 Recovery procedures

Recommendation/comment: Discuss what scripts, if any, should be written in the recovery procedures.