Brainstorming SOPs

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

The developments at the Norwich University Center for Advanced Computing< http://www.nuacc.org/ > continue. A few days before this article went to press, Vermont was alerted to the major risks of heavy rain and wind from Hurricane Sandy< http://www.boston.com/news/weather/2012/10/29/superstorm-glance-vermont/8ndUqwdBJBnmAWQMEKzHiJ/story.html > and the strong possibilities of major electric power outages. Our emergency generator and large-scale uninterruptable power supply have arrived at the University but are not yet installed, so our director, Peter R. Stephenson, PhD, CISSP, CISM, FICAF, LPI, made the decision to bring the systems down on Monday afternoon to prevent catastrophic damage to our virtual systems – crashing virtual pods can result in days of work to re-establish clean virtual machines. We announced that the systems would not be available to support the electronic classrooms that are used for distance-education courses managed by our College of Graduate and Continuing Studies< http://graduate.norwich.edu/ >.

We've been working on formalizing our operations documentation, so a group of us including senior student Jacob Berry as our scribe, met to brainstorm about the structure of standard operating procedures (SOPs). What follows is my interpretation of our discussions; I hope that the ideas will be useful to others and that we can stimulate discussion and information sharing that can help us all improve our SOPs.

The first issue for all SOPs is that we need a unique name, including a sequence number that immediately helps put the SOP in the right context. For example, if our procedures have six sections, and continuing operations are in section 4, then all the operations procedures will be numbered as 4.n (4.1, 4.2, etc.).

Each SOP should include a statement of its purpose. Why do we need this procedure? What does it enable us to do that we can't do without it? This approach is based on the operations credo that every SOP must materially affect our operations.

We need to define the scope of our SOP. What systems and components are involved? For example, which hardware? Which software? Which networks? Which services (such as courses)? Which customers (or groups of customers) are affected (e.g., students in a specific college of the University?

Who are the responsible staff members affected by this SOP? These identities must be role-based and name titles, not personal names. Three classes of people affected by a SOP are

- Those who *authorize* action according to the SOP;
- People who *act* on the SOP;
- People who should be *informed* (e.g., clients, suppliers…) as part of the SOP.

A useful component of any SOP is the critical-path analysis< http://www.mindtools.com/critpath.html > which shows where a procedure fits in the larger schema of operations (e.g., "this SOP is part of the business-continuity section"). What must be done before we can engage this procedure? What sequence of steps (processes) must be followed

to complete the SOP? Which processes can run in parallel within the SOP? What are the possible next steps we might undertake after we complete this SOP?

The SOP must detail all the processes, with explicit numbering to allow everyone in the team to refer to the same process without ambiguity. The processes all have to stipulate what we have to do and how we tell if our process has completed successfully. In addition, we must define how to respond if a process did not work as planned.

OK, so that was a good start.

We continued our discussion with some notes on possible status levels that could be useful in our operations. The primary goal of defining a set of status levels is to improve communications among the operations staff and with customers. Each status level must define how to decide to change from one level to another. The metrics for our Center include the likelihood of degraded quality of service (QoS) or the actual degraded QoS. We settled on a preliminary sketch of four levels and our notes are reasonably clear:

- Green (Normal administration team)
    - No likelihood of degraded QoS
    - Systems are fully operational
- Yellow
    - Low likelihood of degraded QoS
    - Heightened alert to monitor situations
    - No other actions required
    - Who's involved: Normal administration team
- Orange
    - High/Medium likelihood of degraded QoS
    - Growing risk of failure
    - Performing actions to prepare for failure
    - QoS not yet degraded
    - Who's involved: Computer Emergency Response Team (CERT) monitoring and planning to assure business continuity or to safeguard equipment
- Red
    - QoS is degraded
    - Systems are at high levels of failure
    - Operational issues
    - Systems off
    - Whole class room fails
    - Who's involved: CERT actively responding to situation to safeguard equipment and assure speedy restoration of QoS.

Another short discussion concerned defining several out-of-band communications tailored to client preferences. Because we may experience downtime, we choose to use communications that don't depend on continued operations of the Center. Ideas include e-mail, short-message service (SMS) text alerts to mobile devices, a Webpage (possibly using Facebook), and Twitter. Clients would choose any or all of these channels as they see fit.

Finally, we tentatively resolved on a summary definition of who should be in our CERT: the Director, the Associate Director (me), all senior team members, and all lead administrators.

That's the status for now; I'll keep you posted on anything interesting that comes up as we progress.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *