

Operating and Security Standards for Mainframes, Open Systems, and Telecommunications (Part 3 of 3)



By [Leo Wrobel](#)

Date: Dec 22, 2006

[Return to the article](#)

Leo Wrobel concludes his series on developing standards documents with some specific suggestions on departments and phrasing that should be addressed in your standards

We conclude this series with more tips for IT managers who need to develop operating and security standards documents. By the end of reading this series, you should have created a handy "audroes checklist" of importa items to include in your standards

Quick Review

First, let's review the main points from the two previous articles in this seri

- A standards document can be designed as an integral part of the disaster recovery plan. However, it's better to build your standards completely separately from the recovery plan, because standards and disaster recovery deal with different although related issues.
- The standards document is not intended to be a list of emergency procedures. It's signed to mandate changes in the day-to-day conduct of your business, in order to prevent disasters from occurring and/or to ensure that your recovery plan executes gracefully
- The standards document should be written with the support and participation of all departments that will have to work with the final standards
- Some standards apply equally to mainframes, open systems, and telecommunications environments. A good example is standards for wiring, such as the use of fire-retardant cable
- Outside specialists are available who will work without a contract or any prearrangements, and will respond in the event that your equipment gets wet, burned, damaged by smoke, or sabotaged. Contact information for such specialists should be written into your standards document. Such preparations cost nothing, and using this sort of specialist occurs only *after* a disaster presumably, after your business-interruption insurance kicks in.

Now that you're back in standards mode, let's consider the operational standardtion of your standards document. Operational standards include many of the changes you should be considering *now* in your working environment, to ensure that your recovery plan executes gracefully

Standards for Personnel Notification

Developing notification and response procedures for various types of disasters can be a complicated proposition. For example, if a major piece of equipment fails, presumably your IT team would be the principal respondents responsible for restoration of that equipment. However, if the entire building is gone, IT essentially takes a supporting role, directed by the executive management team (EMT) and coordinating with other teams. Your operating standards should specify this distinction and identify responsible personnel by function, rather than by name, in case of employee turnover.

While this specification is a necessary part of the recovery plan, a separate standard is necessary to make such procedures part of your company policy and assign the persons responsible for keeping the plan up to date. Stated another way, if the plan says, "Grab the personnel list and call everyone back to work," it makes the automatic assumption that such a list exists, and that it's accurate

Your standards should consider that notification of an emergency might not come from anyone in your chain of command. More likely, notification will come from someone such as a security guard, facilities manager, or perhaps even the fire department. Carefully consider how your information flows during the early notification phase. For example, if a security guard is making rounds late at night and discovers a door kicked in and a critical server stolen, will he or she know to notify you directly? As you consider this issue, remember that most building security organizations keep some type of a log or call-out book. Even if these employees are outsourced, they will undoubtedly report (eventually) to someone upstream, internal to your company. Your written procedures should spell out who to call if something unusual happens after hours.

You don't have to reinvent the wheel. Identify the procedure and write yourself into it. Then, in your standard document, specify what you did. Be sure that you are part of the building's fire and security personnel procedure, so that they know to call you at the first hint of trouble.

Standards for Emergency Responders

Once you've been notified of an emergency, and after your people arrive on the scene, it will be necessary to make a quick determination as to whether the damage is enterprise-wide (something that involves multiple departments) or is confined to your department. The procedures you will follow in response will be based in large part on an initial assessment. For example, if a power supply goes out in a router or multiplexer, the damage may well affect the company as a whole, but the response will be coordinated principally by technical support rather than by the corporate response team. Therefore, you will need a standard on how often to file reports upstream on your progress in mitigating the problem.

The technical support response team will keep the executive management team or other corporate entity apprised as to the status of the recovery, but basically will act on its own to rectify any problems confined to the technical area of responsibility. This team will also be expected to coordinate with other teams as necessary, of course. For example, the facilities group would be consulted in matters of power issues or common facilities. Depending on the situation, eventually many other teams may be involved in the restoration effort.

On the other hand, if the disaster is more global in nature, such as fire, earthquake, flood, tornado, etc., the technical support team (MIS, open systems, telecommunications, and so on) will act in the "supporting cast" role, taking their direction directly from the EMT.

In either case, the ability to report upstream to the EMT is necessary. Consider including checklists and cheat sheets in your standards document. [Figures 1](#) and [2](#) show some examples.) These lists can be updated periodically to affect changes in technology, or can be written in a more generic fashion. The keys to identify tasks and responsible positions in advance, and then provide some guidance on the nature of those person's responsibilities.

The image shows a document titled "Initial Response Checklist" with several sections for immediate actions. The sections include: "1. Notify the EMT", "2. Notify the Corporate Response Team", "3. Notify the Facilities Group", "4. Notify the Security Guard", "5. Notify the Fire Department", "6. Notify the Police", "7. Notify the Insurance Company", "8. Notify the Vendor", "9. Notify the Customer", "10. Notify the Media", "11. Notify the Public", "12. Notify the Government", "13. Notify the Industry", "14. Notify the Community", "15. Notify the World".

Figure 1 Documents like this tell the first responder what steps to take immediately

The image shows a form titled "Recovery Process" with a flowchart and a list of tasks. The flowchart starts with "Initial Response" and leads to "Recovery Process". The tasks listed are: "1. Notify the EMT", "2. Notify the Corporate Response Team", "3. Notify the Facilities Group", "4. Notify the Security Guard", "5. Notify the Fire Department", "6. Notify the Police", "7. Notify the Insurance Company", "8. Notify the Vendor", "9. Notify the Customer", "10. Notify the Media", "11. Notify the Public", "12. Notify the Government", "13. Notify the Industry", "14. Notify the Community", "15. Notify the World".

Figure 2 Forms prepared in advance can speed the recovery process and prevent the potential confusion of handwritten notes or phone messages

Suggested Standards

The following sections provide some basic standards that would apply to most types of organizations. If you decide to add these standards to your standards document, remember to customize the phrasing and content to fit the needs of your organization and its individual teams.

Human Resources

The human resources team will be responsible for the following:

- Providing a representative at the EMT headquarters
- Notifying families of injured personnel and explaining the benefits program(s)
- Obtaining temporary personnel during the recovery operation
- Providing the EMT with input as to which employees will be required to work during recovery, versus those required to stay home.
- Providing employee home addresses if needed during the recovery operation

Building Facilities

The building facilities team will be responsible for the following:

- Providing a representative at the EMT headquarters
- When local authorities such as police and fire departments need access to the building, providing guidance related to the existence of unique preventive measures such as UPS, special power, automatic locking doors, card key entries, and so on
- Overall assessment of investigation of the cause of the disaster, coordinating with all departments, and including but not limited to the following areas:
 - Architectural
 - Utilities
 - Electrical
 - Environmental (HVAC)
- Managing building repairs and reconstruction activities, including but not limited to the following:
 - Disposal of damage residue
 - Setup of temporary recovery-headquarters location
 - Setup of other temporary work locations

Finance

The finance team will be responsible for the following:

- Providing a representative at the EMT headquarters
- Alerting appropriate corporate and company financial departments
- Providing immediate emergency credit arrangements, petty cash, and travel advance
- Communicating with federal, state, and local taxing authorities
- Providing the EMT and insurance carriers with an approximate estimate of "lost" or destroyed negotiable items or equipment.

Risk Management

The risk management team will be responsible for the following:

- Providing a representative at the EMT headquarters
- Notifying the appropriate insurance companies
- Obtaining "proof of loss" documentation instructions (photographs)
- Obtaining claim-filing instructions from insurance carriers
- Providing guidance regarding actions to be taken during salvage operation
- Processing all insurance claims

- Advising recovery personnel as to the type of records and information to be retained for insurance purposes.

Internal Auditing

The internal auditing team will be responsible for the following

- Filing reports with the EMT headquarters
- Verifying that controls are in place for applications modified to meet limited resources available at the computer backup site.
- Reviewing recovery procedures to ensure assets control during an emergency
- Notifying external auditors, if necessary

Legal or Regulatory

The legal or regulatory team will be responsible for the following

- Providing a representative at the EMT headquarters
- Handling legal issues with next of kin
- Advising recovery personnel on contractual obligations to customers
- Providing copies of contracts destroyed by the disaster.
- Interfacing with media affairs personnel in preparation of public statements

Medical

The medical team will be responsible for the following

- Handling minor medical requests
- Coordinating with local hospitals
- Identifying and locating injured personnel already moved to the hospital
- Assisting in obtaining proper nourishment (and coffee?) for recovery personnel during the recovery operation.
- Ensuring that recovery team members work reasonable, sustainable hours

Administrative

The administrative team will be responsible for the following

- Providing a representative at the EMT headquarters
- Procuring and delivering necessary office supplies for all departments based on a predetermined list of such supplies contained in each department's standards document
- Coordinating with the finance team on necessary approvals using purchase orders "in the pipe" to various suppliers (predefined in the standards document)
- Alerting the post office and forwarding mail as required
- Assisting the facilities team in obtaining security at the affected site
- Establishing an area to accept company deliveries 24 hours a day

Public Relations

The public relations team will be responsible for the following

- Providing a representative at the front door of the affected site within one hour, to handle the inevitable media coverage.
- Coordinating radio and/or TV announcements to notify employees as to where they should report.
- Securing an official company statement from the EMT within 30 minutes. Delivering this official statement to the media both verbally and in writing
- Attempting to minimize any adverse publicity. Suggested behavior:
 - Be sincere.
 - Do not wear sunglasses

- Don't be evasive
- Keep to the company line.
- Coordinating and chairing all press conferences
- Directing, monitoring, and controlling photographers and news crews
- Developing recovery-progress notifications for publication

Transportation/Travel

The transportation/travel team will be responsible for the following:

- Arranging all air and ground transportation
- Providing courier coordination and scheduling
- Obtaining hotel accommodations

Summary

These standards represent only the tip of the iceberg, but they should give you an idea of what a standards document should contain and who it should address. The actual document probably won't contain bulleted lists, but rather detailed information. Then again, depending on the level of documentation your company expects to see, maybe bulleted lists are the best way to go. The typical documents I've seen contain phrasing like the following:

Within 30 minutes of declaration of a disaster, the public relations department will provide a knowledgeable employee, director level or higher (preferably a vice president) at the site of the affected facility. This individual will secure a prepared statement from the EMT via fax, or, if fax is not available, via email or Blackberry. Absent such a statement being available, the responsible individual will read the generic prepared statement in the public relations standards document (stating that the company has implemented its disaster recovery plan and that the situation is under control, etc.) and await a more detailed statement and further instructions from the EMT.

The important thing is to think about these situations beforehand, and then integrate the planning into your day-to-day business. That's why they're *operating* standards.

To recap and summarize:

- Look carefully at your notification procedures and make sure that if something happens when you or your subordinates are not around, you'll be notified properly
- Pay attention to *how* you're notified. You should be included in the procedures for security personnel
- Set up support that's appropriate to the type of disaster you're evaluating where it's confined to a specific department or building-wide, as this will directly affect your response in the opening hours following a disruption.
- Define responsibilities by team or department. Involve all relevant departments
- Run your final standards by your auditors, legal and regulatory group(s), facilities department, and executive management for final benediction and to ensure that the standards coordinate well with the company's overall plan.

I hope that these tips help you. Good luck in your pursuits
