PART V.
RISK AND VULNERABILITY ASSESSMENTS

CONTENTS

5(a) Risk Management

5(a)(1) General

What constitutes a work-related injury? Any illness or injury incurred in the course of employment. This includes industrial accidents, of course, but the injury need not result from one specific event. Repetitive stress injuries, such as back strain or carpal tunnel syndrome, are legitimate worker injuries.

In order to reduce accidents it is important to both identify and prevent accidents at the start, but also to immediately report incidents and to learn from them.

There are no reliable accident statistics in Nigeria, and hence other countries are used by way of examples. According to the National Council on Compensation Insurance (NCCI), the average cost per worker compensation claim in 1996 and 1997 was $10,105 (the latest data available). Motor vehicle accidents were the most costly cause of injury, with an average cost per claim of $19,764. The most costly injuries were amputation, carpal tunnel syndrome, and fractures.

Men are more likely to be hurt on the job than women, filing two thirds of "lost time" claims. Men are also more susceptible to traumatic and permanent injuries. Women, by contrast, are more likely to file mental stress and cumulative-injury claims.

Fueled by statistics like these, on-site safety training or safety-management sessions with managers and employees should be viewed as critical. Companies might promote this as a bonus policy feature, and if you're a small company with few safety-management resources, this can be a huge help in reducing injuries and increasing efficiency. From a practical standpoint, companies may view this as loss-control services. If you're a smaller employer, chances are you don't maintain an internal risk management department. There are, however, many independent risk managers and safety consultants who can work with you to implement safety policies — good accident-reporting practices, safety training for employees, and meeting NERC requirements for your industry can help you keep loss time down by having the right procedures (and the right safety record) in place.

Safety should not be something you talk about once a month. Safety should be in everything you do. Employers need to establish a safety culture – practices and policies that can reduce workers injuries from a humanitarian and a financial standpoint. First and foremost in safety management, is a safety committee, a group of managers and workers that discuss aspects of the workplace and what can be done to improve upon safety and health conditions.

The safety committee should be weighted to the side of the workers. They're involved in the day-to-day processes, and can bring ideas to the table on how to make them safer. Involving employees in that kind of forum is extremely important, because they see themselves as being involved in the process and can take that perspective back to the rest of the employees.

5(a)(2) Steps to Risk Assessment

A risk assessment is an important step in protecting your workers and your business, as well as complying with the law. It helps you focus on the risks that really matter in your workplace – the

ones with the potential to cause real harm. In many instances, straightforward measures can readily control risks, for example ensuring spillages are cleaned up promptly so people do not slip, or cupboard drawers are kept closed to ensure people do not trip. For most, that means simple, cheap and effective measures to ensure your most valuable asset - your workforce - is protected.

A risk assessment is simply a careful examination of what, in your work, could cause harm to people, so that you can weigh up whether you have taken enough precautions or should do more to prevent harm. Workers and others have a right to be protected from harm caused by a failure to take reasonable control measures.

Accidents and ill health can ruin lives and affect your business too if output is lost, machinery is damaged, insurance costs increase or you have to go to court. You are legally required to assess the risks in your workplace so that you put in place a plan to control the risks.

To assess the risks in your workplace follow the five steps below:

1. Identify the hazards;
2. Decide who might be harmed and how;
3. Evaluate the risks and decide on precaution;
4. Record your findings and implement them; and
5. Review your assessment and update if necessary.

5(a)(2)(i) Step 1: Identify the Hazards

First you need to work out how people could be harmed. When you work in a place everyday it is easy to overlook some hazards, so here are some tips to help you identify the ones that matter:

- Walk around your workplace and look at what could reasonably be expected to cause harm.
- Ask your employees or their representatives what they think. They may have noticed things that are not immediately obvious to you.
- If you are a member of a trade association, contact them. Many produce very helpful guidance.
- Check manufacturers' instructions or data sheets for chemicals and equipment as they can be very helpful in spelling out the hazards and putting them in their true perspective.
- Have a look back at your accident and ill-health records – these often help to identify the less obvious hazards.
- Remember to think about long-term hazards to health (e.g., high levels of noise or exposure to harmful substances) as well as safety hazards.

5(a)(2)(ii) Step 2: Decide Who Might be Harmed and How

For each hazard you need to be clear about who might be harmed; it will help you identify the best way of managing the risk. That doesn't mean listing everyone by name, but rather identifying groups of people (e.g. 'people working in the storeroom' or 'passers-by').

Remember:

- some workers have particular requirements, e.g. new and young workers, new or expectant mothers and people with disabilities may be at particular risk. Extra thought will be needed for some hazards;
- cleaners, visitors, contractors, maintenance workers etc, who may not be in the workplace all the time;
- members of the public, if they could be hurt by your activities;
- if you share your workplace, you will need to think about how your work affects others present, as well as how their work affects your staff – talk to them; and
- ask your staff if they can think of anyone you may have missed.

In each case, identify how they might be harmed, i.e. what type of injury or ill health might occur. For example, 'shelf stackers may suffer back injury from repeated lifting of boxes.'

5(a)(2)(iii) Step 3: Evaluate the Risks and Decide on Precautions

Having spotted the hazards, you then have to decide what to do about them. The NERC standards require you to do everything 'reasonably practicable' to protect people from harm. You can work this out for yourself, but the easiest way is to compare what you are doing with good practice.

Initially, look at what you're already doing, think about what controls you have in place and how the work is organized. Then compare this with the good practice and see if there's more you should be doing to bring yourself up to standard. In asking yourself this, consider:

- Can I get rid of the hazard altogether?
- If not, how can I control the risks so that harm is unlikely?

When controlling risks, apply the principles below, if possible in the following order:

- try a less risky option (e.g., switch to using a less hazardous chemical);
- prevent access to the hazard (e.g., by guarding);
- organize work to reduce exposure to the hazard (e.g., put barriers between pedestrians and traffic);
- issue personal protective equipment (e.g., clothing, footwear, goggles etc); and then
- provide welfare facilities (e.g., first aid and washing facilities for removal of contamination).

Improving health and safety need not cost a lot. For instance, placing a mirror on a dangerous blind corner to help prevent vehicular accidents is a low-cost precaution considering the risks. Failure to take simple precautions can cost you a lot more if an accident does happen.

Involve staff, so that you can be sure that what you propose to do will work in practice and won't introduce any new hazards.

5(a)(2)(iv) Step 4: Record Your Findings and Implement Them

Putting the results of your risk assessment into practice will make a difference when looking after people and your business.

Writing down the results of your risk assessment, and sharing them with your staff, encourages you to do this. If you have fewer than five employees you do not have to write anything down, though it is useful so that you can review it at a later date if, for example, something changes.

When writing down your results, keep it simple, for example 'Tripping over rubbish: bins provided, staff instructed, weekly housekeeping checks', or 'Fume from welding: local exhaust ventilation used and regularly checked.'

We do not expect a risk assessment to be perfect – but it must be suitable and sufficient. You need to be able to show that:

- A proper check was made;
- You asked who might be affected;
- You dealt with all the obvious significant hazards, taking into account the number of people who could be involved;
- The precautions are reasonable, and the remaining risk is low; and
- You involved your staff or their representatives in the process.

If, like many businesses, you find that there are quite a lot of improvements that you could make, big and small, don't try to do everything at once. Make a plan of action to deal with the most important things first. Health and safety inspectors acknowledge the efforts of businesses that are clearly trying to make improvements.

A good plan of action often includes a mixture of different things such as:

- a few cheap or easy improvements that can be done quickly, perhaps as a temporary solution until more reliable controls are in place;
- long-term solutions to those risks most likely to cause accidents or ill health;
- long-term solutions to those risks with the worst potential consequences;
- arrangements for training employees on the main risks that remain and how they are to be controlled;
- regular checks to make sure that the control measures stay in place; and
- clear responsibilities – who will lead on what action, and by when.

Remember, prioritize and tackle the most important things first. As you complete each action, tick it off your plan.

5(a)(2)(v) Step 5: Review Your Risk Assessment and Update if Necessary

Few workplaces stay the same. Sooner or later, you will bring in new equipment, substances and procedures that could lead to new hazards. It makes sense therefore, to review what you are

doing on an ongoing basis. Every year or so, formally review where you are to make sure you are still improving, or at least not sliding back.

Look at your risk assessment again. Have there been any changes? Are there improvements you still need to make? Have your workers spotted a problem? Have you learned anything from accidents or near misses? Make sure your risk assessment stays up to date.

When you are running a business, it's all too easy to forget about reviewing your risk assessment – until something has gone wrong and it's too late. Why not set a review date for this risk assessment now? Write it down and note it in your diary as an annual event.

During the year, if there is a significant change, don't wait: check your risk assessment and where necessary, amend it. If possible, it is best to think about the risk assessment when you're planning your change – that way you give yourself more flexibility.

5(a)(2)(vi) Sensible Risk Management Tips

Risk management should be about practical steps to protect people from real harm and suffering – not bureaucratic back covering. If you believe some of the stories you hear, health and safety is all about stopping any activity that might possibly lead to harm. This is not the proper vision of sensible health and safety – rather the focus should be on saving lives, not stopping them. Organizations must seek a balance between the unachievable aim of absolute safety and the kind of poor management of risk that damages lives and the economy.

Don't overcomplicate the process. In many organizations, the risks are well known and the necessary control measures are easy to apply. You probably already know whether, for example, you have employees who move heavy loads and could harm their backs, or where people are most likely to slip or trip. If so, check that you have taken reasonable precautions to avoid injury.

If you run a small organization and you are confident you understand what's involved, you can do the assessment yourself. You don't have to be a health and safety expert.

If you work in a larger organization, you could ask a health and safety advisor to help you. If you are not confident, get help from someone who is competent. In all cases, you should make sure that you involve your staff or their representatives in the process. They will have useful information about how the work is done that will make your assessment of the risk more thorough and effective. But remember, you are responsible for seeing that the assessment is carried out properly.

When thinking about your risk assessment, remember:

- a hazard is anything that may cause harm, such as chemicals, electricity, working from ladders, an open drawer etc; and
- the risk is the chance, high or low, that somebody could be harmed by these and other hazards, together with an indication of how serious the harm could be.

Some frequently asked questions:

1. What if the work I do varies a lot, or I (or my employees) move from one site to another?
   a. Identify the hazards you can reasonably expect and assess the risks from them. This general assessment should stand you in good stead for the majority of your work. Where you do take on work or a new site that is different, cover any new or different hazards with a specific assessment. You do not have to start from scratch each time.
2. What if I share a workplace?
   a. Tell the other employers and self-employed people there about any risks your work could cause them, and what precautions you are taking. Also, think about the risks to your own workforce from those who share your workplace.
3. Do my employees have responsibilities?
   a. Yes. Employees have legal responsibilities to co-operate with their employer's efforts to improve health and safety (eg they must wear protective equipment when it is provided), and to look out for each other.
4. What if one of my employee's circumstances change?
   a. You'll need to look again at the risk assessment. You are required to carry out a specific risk assessment for new or expectant mothers, as some tasks (heavy lifting or work with chemicals for example) may not be appropriate. If an employee develops a disability then you are required to make reasonable adjustments. People returning to work following major surgery may also have particular requirements. If you put your mind to it, you can almost always find a way forward that works for you and your employees.
5. What if I have already assessed some of the risks?
   a. If, for example, you use hazardous chemicals and you have already assessed the risks to health and the precautions you can consider them 'checked' and move on.

Safety risk assessments, to the maximum extent feasible:

1. Are scientifically objective.
2. Are unbiased.
3. Include all relevant data available.
4. Employ default or conservative assumptions only if situation-specific information is not reasonably available. The basis of these assumptions must be clearly identified.
5. Distinguish clearly as to what risks would be affected by the decision and what risks would not.
6. Are reasonably detailed and accurate.
7. Relate to current risk or the risk resulting from not adopting the proposal being considered.
8. Allow for unknown and/or unquantifiable risks.

The principles to be applied when preparing safety risk assessments are:

1. Each risk assessment should first analyze the two elements of risk: severity of the hazard and likelihood of occurrence. Risk assessment is then performed by comparing the combined effect of their characteristics to acceptable criteria as determined in the plan.

2. A risk assessment may be qualitative and/or quantitative. To the maximum extent practicable, these risk assessments will be quantitative.
3. The selection of a risk assessment methodology should be flexible.
4. Basic assumptions should be documented or, if only bounds can be estimated reliably, the range encompassed should be described.
5. Significant risk assessment assumptions, inferences, or models should:
   a. Describe any model used in the risk assessment and make explicit the assumptions incorporated in the model.
   b. Identify any policy or value judgments.
   c. Explain the basis for choices.
   d. Indicate the extent that the model and the assumptions incorporated have been validated by or conflict with empirical data.
6. All safety risk assessments should include or summarize the information gathered. This record should be maintained by the organization performing the assessment.

5(a)(3) Safety Risk Management Committees

A safety risk management committee can provide a valuable service to the organization for safety risk management planning. It can meet periodically to exchange risk management ideas and information. The committee can provide advice and counsel to the managers when requested.

The Safety Risk Management Committee provides a communication and support team to supplement the overall risk analysis capability and efficiency of key managers. The Committee supports safety risk management activities. It provides advice and guidance, upon request from responsible program offices, to help them fulfill their authority and responsibility to incorporate safety risk management as a decision-making tool. It serves as an internal vehicle for risk management process communication, for coordination of risk analysis methods, and for use of common practices where appropriate. This includes, but is not limited to:

1. Continuing the internal exchange of risk management information.
2. Fostering the exchange of risk management ideas and information to avoid duplication of effort.
3. Providing risk analysis/management advice and guidance.
4. Identifying and recommending needed enhancements to risk analysis/management capabilities and/or efficiencies upon request.
5. Maintaining a risk management resources directory that includes:
   a. Risk methodologies productively employed,
   b. Specific internal risk analysis/management expertise by methodology or tool and organizational contact point(s), and
   c. A central contact point for resource identification assistance.
6. Encouraging the establishment of a directory of safety information resources via the Internet.
7. Assisting in the identification of suitable risk analysis tools and initiate appropriate training in the use of these tools.

5(b) Crisis Management

Crisis prevention is very important for small public entities, companies and nonprofit organizations. Small organizations often have fewer resources to draw on when a crisis erupts, and insurance and other risk financing tools may not be an available due to the organization's meager financial resources. But every organization, from the smallest to the largest can and should take steps to prevent the preventable and prepare for the unavoidable. The key is to select the strategies that appeal to your organization and best suit your situation. Once you've undertaken some activities, your organization will be that much more fortified to withstand a crisis.

Crisis management requires your investment of time and common sense, rather than a large budget. You do what you can, as you can, keeping the final goal of preserving your vital mission at the forefront. Consider your organization as a physician considers a patient. Check your nonprofit's vital signs — the ones that enable your organization to fulfill its mission by meeting critical community and citizen/customer/client needs — to establish a baseline for future diagnosis. When you detect an aberration, determine the source, identify treatment methods, apply the methods and evaluate the results. Regular checkups should be scheduled to monitor the organization's vital signs (e.g., funding stream, cash flow, employee and volunteer turnover rates, past incidents, and losses and lawsuits). This process will make a critical difference in your organization's future health.

If your organization is healthy, determine what you can do to keep it that way for a long term. However, if you find weaknesses, you'll need to assess the symptoms, make a diagnosis and begin a treatment plan to cure its ailments so that it can thrive or, at the very least, ease the symptoms to enable it to survive. Weaknesses might exist in financial management, human resources, fund raising or volunteer management. The symptoms could manifest as uneven cash flow; a sharp increase in formal grievances; a complaint from a major constituency, investor or donor; or a steep reduction in volunteer hours. The financial treatment plan could involve purposefully delaying the launch of a new program to coincide with your funding cycle or applying for a line of credit. The human resources treatment plan might be to revise the staff handbook and re-train supervisors on your agency's policies and procedures. The volunteer management plan might involve identifying ways to involve volunteers more deeply in projects that are vital to the realization of your mission, or providing a wider range of opportunities for your volunteer work force.

If possible, you'll want to make gradual changes, starting with the ones that will bring your organization the most benefits. You don't want the treatment to cause more damage than the disease. Instead of forcing a mountain of new policies and procedures on a staff accustomed to an informal work environment, which could send key staff running for the want ads, begin by looking at what works and what's missing.

As a leader who wants a healthier entity, company or nonprofit, visualize what the organization would look like if it were strong and fortified to survive crises. Then divide and conquer the tasks required to reach your goal. How much less stressful this will be on you and your staff — and more do-able than thinking: OK, today I'm writing a crisis management plan and putting safety initiatives into practice and — and — and — or the place will fall apart tomorrow. The

critical difference between success and failure is how you approach crisis management. Ease into making your organization healthier and more likely to avoid a preventable crisis and survive the one fated to occur, or you and your staff risk burnout without completing the job.

Another strategy for getting "buy-in" from personnel is to involve a diverse group of people in your crisis planning activities. If there are nay-sayers in your agency, why not get them involved in the process of identifying the crisis risks you want to focus on and determining the strategies you'll use to address these risks? If they are part of the problem-solving process, you can turn them into ambassadors for the strategies developed by the group, even when these strategies include new policies and procedures.

First, create a comprehensive directory of the organization's staff, board and key volunteers. Include home addresses, phone/fax/wireless/beeper numbers, as well as emergency contact information. Distribute the list to employees and keep copies off site, as well as in your offices. Update and redistribute the directory annually (perhaps the first business day in January or the first day of your fiscal year) or more often if you have a high turnover rate.

Next, maintain a backup of your computer file server, key databases, and financial files. Update the backup weekly (at least) and store a copy off site or on site in a fireproof safe.

Then, conduct an inventory of your nonprofit's assets. Include equipment, furniture, databases, records and anything else you need to fulfill your mission. Your inventory should include brand names, model numbers, location, purchase price and other key details necessary for insurance claims and replacement. Store a copy of the inventory on site (preferably in a fireproof safe) and off site.

Finally, identify an attorney licensed in your state who you can call upon from time to time for advice and assistance. (If your nonprofit can't afford to pay a monthly retainer or an hourly rate, consider soliciting bids from prominent law firms, emphasizing the charitable work of your agency. Don't be surprised if you receive proposals offering pro bono or dramatically discounted legal services).

For many small organizations it makes sense to convene one group to develop a crisis management plan for the organization and a second group that will serve as the nonprofit's "crisis response team." The crisis-planning group should be diverse and include people in the organization who fully understand the risks your operation faces. For example, if you own a building, including the person responsible for maintenance on your crisis planning team can help ensure that building-related hazards that could cause a crisis will be identified and addressed. Including the director of volunteers might enable the team to spot a volunteer-related hazard looming on the horizon.

A crisis response team is the group of people who coordinate your nonprofit's reaction and response to a crisis. The composition of an organization's crisis response team will vary based on a wide range of factors, including: the size of the organization, the nature of the products or services provided, the likely sources of crisis in the organization, and the organization's prior experience responding to a crisis. For example, in an organization with more than 50 staff, the

crisis response team may include a handful of key department heads plus the CEO. In an organization with fewer than 10 paid staff, the crisis response team may include one or more board members, a couple of staff and outside professional advisors.

The composition of a crisis response team will vary with respect to the products and services that you offer. A team at an environmental advocacy group will differ from the team that responds to a crisis at a daycare center. In the former, the team may include an experienced lobbyist and an environmental scientist. In the latter, the team may include the organization's retained counsel, an expert on child-abuse prevention or playground safety, and parents of enrolled children.

The likely sources/causes of crisis in the organization should also be considered in forming a crisis response team. Is the organization more likely to face a crisis stemming from allegations of client/staff mistreatment or a crisis caused by inadequate financial resources? The ranking of crisis risks will suggest areas of expertise and training that may be required during a crisis and individuals with special talents or expertise may be identified as necessary members of the crisis response team. If your public entity, company or nonprofit has successfully weathered a crisis in the past, you'll want to include the people who were effective in addressing that situation on your crisis response team.

5(c) Vulnerability Assessments

A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system or organization. Examples of systems for which vulnerability assessments are performed include, but are not limited to, nuclear power plants, hydroelectric power plants, information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems. Vulnerability assessments can be conducted for small businesses to large regional infrastructures.

A vulnerability assessment has many things in common with a risk assessment. Assessments are typically performed according to the following steps:

1. Cataloging assets and capabilities (resources) in a system.
2. Assigning quantifiable value (or at least rank order) and importance to those resources.
3. Identifying the vulnerabilities or potential threats to each resource.
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources.

Classical risk analysis is principally concerned with investigating the risks surrounding physical plant (or some other object), its design, and operations. Such analyses tend to focus on causes and the direct consequences for the studied object. Vulnerability analyses, in contrast, focuses both on consequences for the object itself and on primary and secondary consequences for the surrounding environment. It also concerns itself with the possibilities of reducing such consequences and of improving the capacity to manage future incidents. In general, a vulnerability analysis serves to categorize key assets and drive the risk management process.

Energy utilities should routinely perform vulnerability assessments to better understand threats and vulnerabilities, determine acceptable levels of risk, and stimulate action to mitigate identified

vulnerabilities. According to the U.S. Department of Energy, the direct benefits of performing a vulnerability assessment include:

- **Build and broaden awareness.** The assessment process directs senior management's attention to security. Security issues, risks, vulnerabilities, mitigation options, and best practices are brought to the surface. Awareness is one of the least expensive and most effective methods for improving the organization's overall security posture.
- **Establish or evaluate against a baseline**. If a baseline has been previously established, an assessment is an opportunity for a checkup to gauge the improvement or deterioration of an organization's security posture. If no previous baseline has been performed (or the work was not uniform or comprehensive), an assessment is an opportunity to integrate and unify previous efforts, define common metrics, and establish a definitive baseline. The baseline also can be compared against best practices to provide perspective on an organization's security posture.
- **Identify vulnerabilities and develop responses.** Generating lists of vulnerabilities and potential responses is usually a core activity and outcome of an assessment. Sometimes, due to budget, time, complexity, and risk considerations, the response selected for many of the vulnerabilities may be non-action, but after completing the assessment process, these decisions will be conscious ones, with a documented decision process and item-by-item rationale available for revisiting issues at scheduled intervals. This information can help drive or motivate the development of a risk management process.
- **Categorize key assets and drive the risk management process.** An assessment can be a vehicle for reaching corporate-wide consensus on a hierarchy of key assets. This ranking, combined with threat, vulnerability, and risk analysis, is at the heart of any risk management process. For many organizations, the Y2K threat was the first time a company-wide inventory and ranking of key assets was attempted. An assessment allows an organization to revisit that list from a broader and more comprehensive perspective.
- **Develop and build internal skills and expertise.** A security assessment, when not implemented in an "audit" mode, can serve as an excellent opportunity to build security skills and expertise within an organization. A well-structured assessment can have elements that serve as a forum for cross-cutting groups to come together and share issues, experiences, and expertise. External assessors can be instructed to emphasize "teaching and collaborating" rather than "evaluating" (the traditional role). Whatever an organization's current level of sophistication, a long-term goal should be to move that organization towards a capability for self-assessment.
- **Promote action.** Although disparate security efforts may be underway in an organization, an assessment can crystallize and focus management attention and resources on solving specific and systemic security problems. Often, the people in the trenches are well aware of security issues (and even potential solutions) but are unable to convert their awareness to action. An assessment provides an outlet for their concerns and the potential to surface these issues at appropriate levels (legal, financial, executive) and achieve action. A well-designed and executed assessment not only identifies vulnerabilities and makes recommendations, it also gains executive buy-in, identifies key players, and establishes a set of cross-cutting groups that can convert those recommendations into action.

- **Kick off an ongoing security effort.** An assessment can be used as a catalyst to involve people throughout the organization in security issues, build cross-cutting teams, establish permanent forums and councils, and harness the momentum generated by the assessment to build an ongoing institutional security effort. The assessment can lead to the creation of either an actual or a virtual (matrixed) security organization.

The assessment methodology consists of 10 elements:

1. Network architecture;
2. Threat environment;
3. Penetration testing;
4. Physical security;
5. Physical asset analysis;
6. Operations security;
7. Policies and procedures;
8. Impact analysis;
9. Infrastructure interdependencies; and
10. Risk characterization.

5(c)(1)Network Architecture

This element provides an analysis of the information assurance features of the information network(s) associated with the organization's critical information systems. Information examined should include network topology and connectivity (including subnets), principal information assets, interface and communication protocols, function and linkage of major software and hardware components (especially those associated with information security such as intrusion detectors), and policies and procedures that govern security features of the network. Procedures for information assurance in the system, including authentication of access and management of access authorization, should be reviewed. The assessment should identify any obvious concerns related to architectural vulnerabilities, as well as operating procedures.

Existing security plans should be evaluated, and the results of any prior testing should be analyzed. Results from the network architecture assessment should include potential recommendations for changes in the information architecture, functional areas and categories where testing is needed, and suggestions regarding system design that would enable more effective information and information system protection.

Three techniques are used in conducting the network architecture assessment:

1. Analysis of network and system documentation during and after the site visit;
2. Interviews with facility staff, managers, and Chief Information Officer; and
3. Tours and physical inspections of key facilities.

5(c)(2) Threat Environment

Development of a clear understanding of the threat environment is a fundamental element of risk management. When combined with an appreciation of the value of the information assets and systems, and the impact of unauthorized access and subsequent malicious activity, an

understanding of threats provides a basis for better defining the level of investment needed to prevent such access.

The threat of a terrorist attack to the electric power infrastructure is real and could come from several areas, including physical, cyber, and interdependency. In addition, threats could come from individuals or organizations motivated by financial gain or persons who derive pleasure from such penetration (e.g., recreational hackers, disgruntled employees). Other possible sources of threats are those who want to accomplish extremist goals (e.g., environmental terrorists, antinuclear advocates) or embarrass one or more organizations.

This element should include a characterization of these and other threats, identification of trends in these threats, and ways in which vulnerabilities are exploited. To the extent possible, characterization of the threat environment should be localized, that is, within the organization's service area.

5(c)(3) Penetration Testing

The purpose of network penetration testing is to utilize active scanning and penetration tools to identify vulnerabilities that a determined adversary could easily exploit. Penetration testing can be customized to meet the specific needs and concerns of the utility. In general, penetration testing should include a test plan and details on the rules of engagement (ROE). It should also include a general characterization of the access points to the critical information systems and communication interface connections, modem network connections, access points to principal network routers, and other external connections. Finally, penetration testing should include identified vulnerabilities and, in particular, whether access could be gained to the control network or specific subsystems or devices that have a critical role in assuring continuity of service.

Penetration testing consists of an overall process for establishing the ground rules or ROE for the test; establishing a white cell for continuous communication; developing a format or methodology for the test; conducting the test; and generating a final report that details methods, findings, and recommendations.

Penetration testing methodology consists of three phases: reconnaissance, scenario development, and exploitation. A one-time penetration test can provide the utility with valuable feedback; however, it is far more effective if performed on a regular basis. Repeated testing is recommended because new threats develop continuously, and the networks, computers, and architecture of the utility are likely to change over time.

5(c)(4) Physical Security

The purpose of a physical security assessment is to examine and evaluate the systems in place (or being planned) and to identify potential improvements in this area for the sites evaluated.

Physical security systems include access controls, barriers, locks and keys, badges and passes, intrusion detection devices and associated alarm reporting and display, closed-circuit television (assessment and surveillance), communications equipment (telephone, two-way radio, intercom, cellular), lighting (interior and exterior), power sources (line, battery, generator), inventory control, postings (signs), security system wiring, and protective force. Physical security systems are reviewed for design, installation, operation, maintenance, and testing.

The physical security assessment should focus on those sites directly related to the critical facilities, including information systems and assets required for operation. Typically included are facilities that house critical equipment or information assets or networks dedicated to the operation of electric or gas transmission, storage, or delivery systems. Other facilities can be included on the basis of criteria specified by the organization being assessed. Appropriate levels of physical security are contingent upon the value of company assets, the potential threats to these assets, and the cost associated with protecting the assets. Once the cost of implementing/maintaining physical security programs is known, it can be compared to the value of the company assets, thus providing the necessary information for risk management decisions. The focus of the physical security assessment task is determined by prioritizing the company assets; that is, the most critical assets receive the majority of the assessment activity

At the start of the assessment, survey personnel should develop a prioritized listing of company assets. This list should be discussed with company personnel to identify areas of security strengths and weaknesses. During these initial interviews, assessment areas that would provide the most benefit to the company should be identified; once known, they should become the major focus of the assessment activities.

The physical security assessment of each focus area usually consists of the following:

- Physical security program (general);
- Physical security program (planning);
- Barriers;
- Access controls/badges;
- Locks/keys;
- Intrusion detection systems;
- Communications equipment; and
- Protective force/local law enforcement agency.

The key to reviewing the above topics is not to just identify if they exist, but to determine the appropriate level that is necessary and consistent with the value of the asset being protected. The physical security assessment worksheets provide guidance on appropriate levels of protection.

Once the focus and content of the assessment task have been identified, the approach to conducting the assessment can be either at the “implementation level” or at the “organizational

level." The approach taken depends on the maturity of the security program. For example, a company with a solid security infrastructure (staffing, plans/procedures, funding) should receive a cursory review of these items. However, facilities where the security programs are being implemented should receive a detailed review. The security staff can act upon deficiencies found at the facilities, once reported.

For companies with an insufficient security organization, the majority of time spent on the assessment should take place at the organizational level to identify the appropriate staffing / funding necessary to implement security programs to protect company assets. Research into specific facility deficiencies should be limited to finding just enough examples to support any staffing / funding recommendations.

5(c)(5) Physical Asset Analysis

The purpose of the physical asset analysis is to examine the systems and physical operational assets to ascertain whether vulnerabilities exist. Included in this element is an examination of asset utilization, system redundancies, and emergency operating procedures. Consideration should also be given to the topology and operating practices for electric and gas transmission, processing, storage, and delivery, looking specifically for those elements that either singly or in concert with other factors provide a high potential for disrupting service. This portion of the assessment determines company and industry trends regarding these physical assets. Historic trends, such as asset utilization, maintenance, new infrastructure investments, spare parts, SCADA linkages, and field personnel are part of the scoping element.

Key output from analysis should be graphs that show trends. The historic data analysis should be supplemented with on-site interviews and visits. Items to focus on during a site visit include the following:

- Trends in maintenance expenditures and field staffing;
- Trends in infrastructure investments;
- Historic infrastructure outages;
- Critical system components and potential system bottlenecks;
- Overall system operation controls;
- Use and dependency of SCADA systems;
- Linkages of operation staff with physical and IT security;
- Adequate policies and procedures;
- Communications with other regional utilities;
- Communications with external infrastructure providers; and
- Adequate organizational structure.

5(c)(6) Operations Security

Operations security (OPSEC) is the systematic process of denying potential adversaries (including competitors or their agents) information about capabilities and intentions of the host organization. OPSEC involves identifying, controlling, and protecting generally non-sensitive activities concerning planning and execution of sensitive activities. The OPSEC assessment reviews the processes and practices employed for denying adversary access to sensitive and non-

sensitive information that might inappropriately aid or abet an individual's or organization's disproportionate influence over system operation (e.g., electric markets, grid operations). This assessment should include a review of security training and awareness programs, discussions with key staff, and tours of appropriate principal facilities. Information that might be available through public access should also be reviewed.

5(c)(7) Policies and Procedures

The policies and procedures by which security is administered: (1) provide the basis for identifying and resolving issues; (2) establish the standards of reference for policy implementation; and (3) define and communicate roles, responsibilities, authorities, and accountabilities for all individuals and organizations that interface with critical systems. They are the backbone for decisions and day-to-day security operations. Security policies and procedures become particularly important at times when multiple parties must interact to effect a desired level of security and when substantial legal ramifications could result from policy violations. Policies and procedures should be reviewed to determine whether they (1) address the key factors affecting security; (2) enable effective compliance, implementation, and enforcement; (3) reference or conform to established standards; (4) provide clear and comprehensive guidance; and (5) effectively address the risks.

The objective of the policies and procedures assessment task is to develop a comprehensive understanding of how a facility protects its critical assets through the development and implementation of policies and procedures. Understanding and assessing this area provide a means of identifying strengths and areas for improvements that can be achieved through:

- Modification of current policies and procedures;
- Implementation of current policies and procedures;
- Development and implementation of new policies and procedures;
- Assurance of compliance with policies and procedures; and
- Cancellation of policies and procedures that are no longer relevant, or are inappropriate, for the facility's current strategy and operations

5(c)(8) Impact Analysis

A detailed analysis should be conducted to determine the influence that exploitation of unauthorized access to critical facilities or information systems might have on an organization's operations (e.g., market and/or physical operations). In general, such an analysis would require thorough understanding of: (1) the applications and their information processing; (2) decisions influenced by this information; (3) independent checks and balances that might exist regarding information upon which decisions are made; (4) factors that might mitigate the impact of unauthorized access; and (5) secondary impacts of such access (e.g., potential destabilization of organizations serving the grid, particularly those affecting reliability or safety). Similarly, the physical chain of events following disruption, including the primary, secondary, and tertiary impacts of disruption, should be examined.

The purpose of the impact analysis is to help estimate the impact that outages could have on a utility. Outages in electric power, natural gas, and oil can have significant financial and external

consequences to a utility. The impact analysis provides an introduction to risk characterization by providing quantitative estimates of these impacts so that the utility can implement a risk management program and weigh the risks and costs of various mitigation measures.

5(c)(9) Infrastructure Interdependencies

The term “infrastructure interdependencies” refers to the physical and electronic (cyber) linkages within and among our nation’s critical infrastructures — energy (electric power, oil, natural gas), telecommunications, transportation, water supply systems, banking and finance, emergency services, and government services. This task identifies the direct infrastructure linkages between and among the infrastructures that support critical facilities as recognized by the organization. Performance of this task requires a detailed understanding of an organization’s functions, internal infrastructures, and how these link to external infrastructures.

The purpose of the infrastructure interdependencies assessment is to examine and evaluate the infrastructures (internal and external) that support critical facility functions, along with their associated interdependencies and vulnerabilities.

5(c)(10) Risk Characterization

Risk characterization provides a framework for prioritizing recommendations across all task areas. The recommendations for each task area are judged against a set of criteria to help prioritize the recommendations and assist the organization in determining the appropriate course of action. It provides a framework for assessing vulnerabilities, threats, and potential impacts (determined in the other tasks). In addition, the existing risk analysis and management process at the organization should be reviewed and, if appropriate, utilized for prioritizing recommendations. The degree to which corporate risk management includes security factors is also evaluated.

5(c)(11) Post-Assessment

The post-assessment phase involves prioritizing assessment recommendations, developing an action plan, capturing lessons learned and best practices, and conducting training. The risk characterization element results provide the basis for the post-assessment by providing prioritized lists of recommendations that are ranked by key criteria. The company should take the prioritized lists and validate the recommendations and costs. Recommendations that are low cost or result in cost savings should be singled out for special attention. Other recommendations, however, might require formidable financial resources for implementation and require knowledge of the current company financial situation and posture toward risk.

Each company should carefully evaluate the costs and benefits of each recommendation. Recommendations compared in this section include making trade-offs in improvements in each of the other element areas. For example, which physical security measures should be selected versus changes in policies and procedures and network architecture? These are difficult decisions to make and a risk management framework combined with a diverse group of company decision makers should be a part of this decision making process.

The next step is to develop an action plan that includes timelines, staffing assignments, and budgets to implement the proposed recommendations. Lessons learned should be captured along the way to improve the overall process in the future. Training and other technical support activities, such as workshops, are also appropriate throughout the process.

This Section is reserved for further expansion by NERC as standards are updated in the future and resources expanded on Vulnerability Assessments.