Conducting the Crisis Audit

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Discuss how to conduct a crisis audit

Conducting the Crisis Audit

Why Audit?

In any discussion of safety and well-being, we really want to focus on **prevention** because we understand how much value comes from preparing and preventing a crisis. But it is impossible to plan for every event and to create a perfect environment that will outlast any kind of calamity. In health and safety terms, we regularly undertake hazard assessments in the workplace. A **crisis audit** is no different as we review our environment and see what threats exist, and which of those we can minimize or eradicate through pro-active actions.

An audit makes financial sense, too. If we fix something before it breaks (or breaks down, shorts out, or blows up) we need fewer resources and money than we do to react afterward. Take the case of the light switch that gives you a shock when you turn it off. You know that there is probably a short somewhere and an electrician can locate and fix the problem for his hourly fee plus a service call. Ignoring the short, however, can lead to a fire that destroys part of your building, delays important work, and injures employees. That old expression, "An ounce of prevention is worth a pound of cure," sticks around for a reason!

In order to complete the audit process in manageable pieces, there are different ways to go about it. We recommend the following process, which can be adapted to suit your needs.

Documentation Audit

A documentation audit is a thorough review of all emergency, crisis, safety plans, and hazard assessments that the company has already completed. Some companies have done a lot of crisis management work already; there may be a fire plan, a chemical spill plan, an electrical outage plan, etc. This part of the audit will help to bring it all together in one place and identify gaps that have not been addressed so far.

360-Degree Audit

In the sense that a 360° performance review looks at all influences of an employee's work, this audit is similar. All levels of the organization need to be interviewed, including key external stakeholders and clients. Each stage of the audit concludes with a comprehensive report that includes the steps that need to be taken in order to minimize the risks and threats identified. Each interview needs to be short (especially if it is a big organization, or you'll never finish!), so plan for about twenty minutes per person.

You might look at the list below and think it is too much. However, keep in mind that your senior people are probably unaware of threats that are noticeable to middle and front-line staff, and middle or front line staff are not aware of threats that senior staff will be aware of.

Executive Audit

The auditor will facilitate a session with the company's executive team (typically an entire day) to help them identify and elaborate on vulnerabilities that exist and have the potential to escalate. This often gives a vastly different point of view than what is gleaned from employees, since the executive team may have knowledge of threat from competitors and outside factors (such as organizational, funding, taxation, compliance, and takeover issues) that other members of the company may not have.

Employee Audit

In this stage, information is gathered through interviews with all employees (or at least representatives of each department and committee). The interview approach is to encourage employees to speak freely and to ensure their responses are kept confidential. There is often the potential of employees not reporting all vulnerabilities if they feel that their information will jeopardize their job in any way.

External Audit

These interviews are also best done individually in order to maintain privacy and to encourage open conversation. However, this will depend on the company's relationship with the external clients, the nature of the business, and the company itself. If your company is threatened by something that an external provider can see, then you need to know!

Online Audit

Twenty years ago we would not have bothered with this, but the Internet is a vast resource of information about your company and may hold a lot of information that you did not know was out there in the public realm. This audit has to be conducted by specialists with sophisticated knowledge of data mining, analysis, and interpretation. The audit needs to look at threats to reputation (which can sometimes be found on websites that are set up to complain, as well as places with more subtlety), as well as threats from people trying to breach systems. This report can be useful to the company executive, public relations and communications teams, and information technology staff.

Sample Audit Questions

You'll need to customize the questions you ask to fit the company and what they do. This list is here to start you off.

- Tell me if you notice any threats to safety here at work. How about threats to business continuity?
- If there was an emergency this evening, and you had to report to work offsite tomorrow, do you know how to work remotely?

- Can you perform your job without access to your computer or usual machinery?
- Is there a place designated as an Emergency Operation Center where work can be underway with minimum delay? Have you been there to see if it meets your needs?
- Do you understand your role in an emergency situation? Have you been trained for that role?
- Do you have access to contact information for everyone (internal and external)? How often is it updated?
- If your computer is unavailable, how will you access the information that you need?
- What areas of vulnerability do you see that could lead to a problem? (Use the language of creeping, slow-burn, and sudden crisis as suits the situation.)
- Are confidential documents securely stored and shredded?
- Is security for all remote access to computers and equipment secure?
- Is garbage and recycling (such as the disposal of used manufacturing parts, which could contain proprietary information) secured?
- Do people have highly secure passwords in place to protect information on their computers and cell phones?
- Do people walk away from their desks and leave their desktop open?
- Can phone conversations or meetings be overheard?

Test Your Knowledge

Add your own questions here.

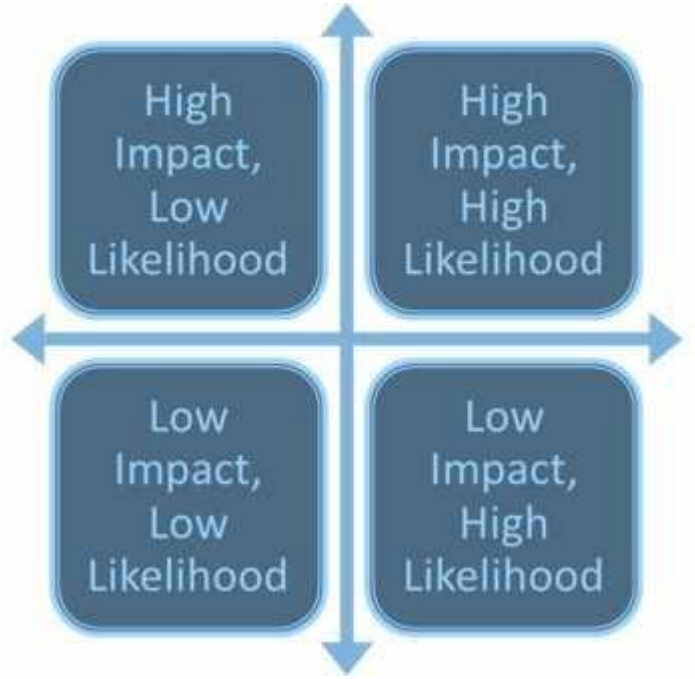
If the company is small, you can probably conduct the audit quite quickly and easily. Even walking around the facility (inside and out) and visiting popular lunch restaurants can reveal a lot.

As we have mentioned, prevention is the best way to manage any crisis, and there may be lots of quick, simple things that can be implemented to mitigate any risks that are identified through these interviews.

Using a Risk Matrix

Reports are intended to be read, but sometimes after the audit is done and reports are submitted, we don't hear anything back. We end up in some kind of limbo, waiting. If your reports have been submitted

to people who appreciate a more visual context, or there are a lot of risks identified and you are trying to decide what needs doing first, you can plot your results on a risk matrix.



Performing a Risk Level Analysis

The Four Categories

Earlier, we offered a matrix for determining priorities and likelihood that a crisis could develop. Another way of looking at this is to conduct a risk level analysis. *(Based on violence response system proposed by Dr. James Turner and Dr. Michael Gelles in "Threat Assessment: A Risk Management Approach")*

Category 1 (Most Severe)

- Available data suggests high risk potential
- Risk has been demonstrated to be severe in the past (high likelihood and high impact)
- Requires major organizational response
- Example: There is a hurricane alert for your area. Damage has been devastating with this type of storm in the past.

Category 2

- Available data suggests high risk potential
- Organization identifies crisis as low likelihood and high impact, but organization should still be prepared
- Requires major organizational response

- Example: There is a hurricane watch for your area, although a storm has never struck your city before.

Category 3

- Available data is insufficient to determine risk potential
- Organization identifies crisis as low likelihood and high impact
- Organization is concerned about the potential effects of the crisis
- Requires moderate to major organizational response
- Example: A bomb threat is called in by an individual who has made false threats before. Security measures make it unlikely that what he says is true.

Category 4 (Least Severe)

- Available data is insufficient to determine risk potential
- Organization identifies crisis as low likelihood and low impact
- Report of risk may be unfounded
- Requires low to moderate organizational response
- Example: There is a rumor that the local telephone company may go on strike.

Further Reading:

✓