Incident Reports – Why, when, and How

Several months ago I got asked by a client if I had any good examples of incident reports that got me thinking about doing a TOM (Tip of The Month) on that topic.

Incident reports come in many sizes, sizes, and colors. There are probably thousands around the world. I really have no idea where incident reports were first used but could assume, you know what happens when we do that! They were first used by police, fire, and or security organizations to document what happen at the scene of whatever kind of event took place. In today’s world they are common place in all types of industries and businesses. They are used as a document describing everything which took place leading up to an incident, during the incident, and the after effects or consequences after the incident is remediated. Typically they are initiated when something happens which is deemed to be out of the normal activities or processes of your organization.

Over the years I have assisted in setting up and teaching subjects like RCFA (Root Cause Failure Analysis) and FMEA (Failure Mode and Effect Analysis. Both are key in problem analysis and also in potential problem prevention processes. And, they use incident reports as a key component for gathering information and using them to solve or prevent the problem from occurring in the future.

The most important component of any incident is the rapid and accurate gathering of the facts. Remember the facts and data related to the incidents are perishable and will not survive very long. You must get it fast and accurately or it will be impossible to accurately determine the root cause of any problem with any accuracy. Think of perishable evidence. It is the same as bringing home a gallon of milk but you don’t have a refrigerator, so you just store it on the kitchen counter. How long do you think it will last? Maybe today, but definitely not into tomorrow. Evidence in an equipment failure will last about as long if you don’t secure it properly and gather the details quickly before things get moved, repaired, or memories are clouded. You need to move quickly and decisively. I would suggest developing some standard reasons to begin the incident reporting process. Here are some examples which should be documented in your SOPs (Standard Operation Procedures)

- Loss of service of critical systems
- Personal injury – employees and or the public
- Major financial costs
- The police or fire officials were called
- The press showed up
- Environmental problems – must report to state or feds
- We had to wake up the “Boss”
- Etc…
I think you get the picture; the major ones should be documented in your SOPs so everyone knows when and how to begin the process. If something wakes you up in the middle of the night or causes you to think about how up-to-date your resume is; then maybe you need to begin the incident documentation process.

I covered the why and when of incident reports so now let’s discuss the how and what of the process. So what evidence and data do you need to collect? A lot depends on what type of incident it is; safety, fire, security or some kind of system or equipment failure. Your forms and the data types will vary for all of the above. The basic rule of thumb is you need all the evidence and facts which will allow you and your team to accurately and completely recreate the events after the dust settles. You’re looking for information which took place during the different phases of the incident.

- What lead up to the incident? What was happening prior the situation occurring?
- What happen during the incident? Who saw what, heard what, or smelled what?
- What happen immediately after the incident? Who did what?
- And lastly, what took place until things were deemed to be “back to normal”?

The process of initiating the incident reporting process should be as automatic as possible. If you have to ask someone if a report should be developed then you are losing time and more than likely losing quality evidence. Your SOPs should be the determining factor during off hours and if managers during the normal work times cannot be reached. Keep in mind that even the SOP does not say we need to do a report; if management determines it is appropriate, one can be started. Below are some suggestions of what needs to be included in your incident reporting.

- Time and date
- Who was involved, who found the problem?
- Pictures, pictures, pictures – remember the evidence will be gone in 24 hours or less
- What was happening prior to the problem?
- Gather all technical data – temperature, pressure, voltage, etc.
- More data is better if you’re not sure capture it anyway

Incident reports are designed to assist with gathering the critical data needed to make critical operational and equipment decisions after the problem which will hopefully assist you in preventing future occurrences. The bottom-line is to gather as many details as possible and take twice as many pictures as possible. When I teach RCFA and FMEA classes I take pictures of an actual incident and then go back to the classroom and project them to the class. Every time I do this I always end up saying, “darn I wish I a picture of that.”

I was going to have an example of an incident report available but it will be easier and more beneficial to you if you just Google incident reports. I found hundreds from all types of industries and organizations.