The IA Consultant’s Toolkit:  
Part 8 – Problem Management 

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

Security Consultant Gordon Merrill continues his series on fundamental tools for IA security consultants – and IA professionals in general. The work is based on some of the papers Mr Merrill wrote during his MSIA Program<http://infoassurance.norwich.edu/> at Norwich University<http://www.norwich.edu> from 2007 through 2008. Everything below is entirely Mr Merrill’s work with minor edits.

* * *

Your success as a contractor in the Information Assurance world will depend on your skills. What will set you apart from other IA professionals will be your soft skills. The Information Assurance Professional Consultant’s Toolkit reviews what C-level executives want to see in order to offer you that contract.

Problem Management

As a consultant you will not be on the receiving end of too many corporate problems with security. Most of your business will be after the big event has happened. That does not mean that you may not be tasked with trying to set up a disaster response and recovery plan for the client for their future.

1.1.1 Incident or Problem?

You cannot have an incident without a problem but you can have problems that have not yet become incidents. That being the case the following will look as incidents just like problems. Incidents may be the result of one or more problem but there will always be a problem at the core.

1.1.2 Proactive or Reactive?

Nearly everyone in IA today agrees that what has been done to date in the industry as far as security has not worked. The need for change in upon us and the only way to change and become more secure is to re-engineer how we do security. That way of thinking is proactive. Companies are either proactive or reactive in how they handle problems as well. If you are called only hours after the company notices a problem they may be proactive. If however you have a company who has known of a problem for some time and has decided to ignore they may be very much reactive and will wait till the problem becomes an incident before making any effort to handle the problem(Stacey). Some of this may be voluntary on their part, but also some of it may be just not enough budgets to fix all the problems so they have to let some go until they get more money or the problem gains a greater priority.
### 1.1.3 Managing Priorities and Solutions

Each company will probably have their own priorities in how they address problems. Their priorities will probably not coincide with yours. That does not mean you need to forget yours or not maintain your own set of priorities. Much like each contract and client you embark on a project with is a project of its own in your business whether or not you lead the project for the client; so to your priorities will be needed to help you focus on finding problems, causes, and solutions.

To solution a security problem the main focus is to find the hole in the security, secure the defenses, and apply a quick fix. That however, is only the beginning. The priorities you maintain personally will now help you examine the situation fully, look for the root cause, and determine a solution. You may find the quick fix is all that is needed to completely eradicate the problem, more realistically you will find the quick fix to be just a patch on the problem until the problem can be fully realized, tested, and resolved across the enterprise (NIST). Your biggest friends through this process will be your priorities and your documentation.

### 1.1.4 Documentation

*Peanuts* had a cartoon once with Snoopy in the bathroom with a very forlorn look on his face which read, “No job is done until the paperwork is done.” The phrase really needs to read …until the paperwork is complete. IT and documentation seem to have a constant ongoing struggle. Usually there is something started or an outline there but in most cases “complete” documentation is hard to find in corporate IT. Part of that overflows into the disaster response and recovery operations. The time to figure out who is responsible for application XYZ and server ABC is not when there is a breach in security it is when you have time to ruin it down and verify information and get phone numbers and emails (Merrill). Part of what you do with a client who has hired you due to a problem may include guiding them through formulating a DR plan. You need to make sure that your documentation for you, your business, and papers going to your client are as complete and professional as possible especially if they may need to look into asking you to help them document.

A judge once said in his court room on a special training weekend about malpractice cases, “If it isn’t written down, it didn’t happen.” Your documentation should be as complete as you would want to see if that was all you were allowed to have in the courtroom to remember a case you worked on twenty years ago (Merrill).

---

**A guide to the project management body of knowledge (PMBOK guide).** 3rd ed. Newtown Square, Pa: Project Management Institute, Inc., 2004


* * *

Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and to six foreign countries. Gordon’s information assurance background has included working for major computer companies like IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. You may contact him by e-mail: Merrill.IA@gmail.com
Gordon Merrill, MSIA, currently lives and works in Tennessee. His career has taken him to 48 of the 50 states and six foreign countries. Gordon’s Information Assurance background has included working for major computer companies like IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant.

Gordon Merrill
Merrill.IA@gmail.com

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>