

Security and Audit: Oil and water?

By Keith G. Parsons

This article looks at the relationship between Security and Audit, and asks, “Do they have to be like oil and water?”

In two previous *ISSA Journal* articles – “Making Management Aware of the Risks” Jan/03, and “Information Systems Security + Technical Services = Together Stronger” Oct/03 – I highlighted the benefits of a cooperative and cohesive partnership between different areas of an organization. Completing a sort of trilogy on this theme, this article looks at the relationship between Security and Audit, and asks “Do they have to be like oil and water?”

I think not. We are all striving for the same results, and this is perhaps truest between Security and Audit. When these two groups work *together* with business and technical partners – internal and external – common ground can often be achieved, ensuring that an effective security posture exists.

Standards, standards, standards

Standards are crucial in today’s complex environments. But there are often conflicts between security standards and audit standards. To minimize these conflicts, first determine how these standards are to be defined, structured, implemented, applied and reviewed to ensure compliance by all personnel. It is well known that compliance is far more cost-effective than enforcement. Having forged professional alliances with my audit colleagues, I have shared with them the victories that come with adopting a plan that can work for everyone, saving our organizations money and grief in the process. Having a mutually agreed to baseline is the key to success.

As a security practitioner you have been tasked by management to “preserve and protect the corporate resource” by keeping the organization safe from the threats, risks and impacts prevalent in a heterogeneous and open IT environment. In cooperation with technical services, operational and business unit co-workers, you accomplish much in developing the security program. The next step requires *sharing* that program with internal and external auditors, and garnering their support to bring it all together. This step is unfortunately often overlooked; but once done, a baseline of standards can now exist for an efficient and workable implementation and

follow through from development to testing to acceptance to implementation, all the way to the post-implementation review – the Audit.

Scenario

One of your business line management teams has requested and received executive approval for the development of a new application to streamline and automate customer ordering, inventory and follow-up service that will be web-based and outsourced to a third party service provider. The security group (i.e., you) has been assigned as part of the project team and the security requirements are quite straightforward:

- Classify the criticality of the data to be processed
- Assess the risks of the data and processes being exported
- Qualify the applicable security components in a network and system design topology
- Conduct an appropriate level of due diligence with the service provider
- Provide lead, guidance and direction to both internal and external project teams

By now some of you reading this are already thinking, “I do this now and still have to deal with the auditors six months after the process has been put into service. So tell me something I can use now.” Okay, here goes....

Bring Audit into the picture now

Whether Audit can join the team now or only get involved at a later stage, their roles and responsibilities will likely be the same. *Find out what they will be looking for and try to work that into your portion of the project plan.* When it is known that something different is required for the new process to work, open a dialogue with Audit and develop an acceptable and authorized deviation strategy so as to pass the audit, although the standard may not exactly be met.

Years ago I was tasked with securing a new Novell LAN covering several locations in different cities for use by a few thousand employees. I worked with the technical and network services people during the planning phase. We developed and agreed upon a consistent level of security end-to-end. During a project meeting I heard a colleague quip, "Audit will probably fail this whole process anyway." Armed with that comment, I made an appointment with the audit group that afternoon.

Got a minute?

On meeting my audit colleague I noticed shelf upon shelf of labeled binders which immediately set my tone for the meeting. Asking if any audit standards were available for Novell LANs, I was promptly handed a rather large binder of about 400 pages and told "this is what must be in place." Several sections in I realized compliance to these standards as written vis-à-vis our project requirements was not going to happen. During the second meeting with Audit, I laid out what the project team had already agreed to and set about to compare the binder standards to a "real world" deployment that would be in compliance. Compromise was alive and well those next few weeks as the paper-based audit standards and the deployment security standards became almost as one. Sure enough, approximately six months after that LAN went into full production the entire process was audited and passed all scrutiny.

Professional to professional

Whenever possible, my security colleagues and I work closely with our Audit colleagues in all phases of a project to ensure consistency and acceptance by all stakeholders. I, like most of you reading this article, am a professional security practitioner, and whether certified in any of the current security disciplines or not, I – like you – take my work very seriously. The same applies to professional auditors who may or may not be certified in their chosen field but who also take their work very seriously. With less resources and shorter time frames, it is in our mutual interests to collaborate and work together toward the same goals.

So rather than oil and water – never mixing, both groups should stand together side-by-side, albeit with different approaches and somewhat different means, focused on the same objectives.

About the Author

Keith G. Parsons, CISSP, CISM is a former Director, Vice-President and President of the ISSA Toronto Chapter and a 40-year veteran within the information technology field, the last 25 in Information and Systems Security. Parsons is principal of his own security consultancy, Kei-Mar & Associates and is a frequent speaker at security conferences, seminars and symposiums. He can be reached at picker1@sympatico.ca.