



Utah ISACA Spring Seminar

Developing and Implementing an Organizational Risk Assessment Process

- Speaker:** Steven F. Fox
When: May 22, 2008
Time: 8:30 to 4:30 (7 CPE Hours)
Where: Thanksgiving Point – Amber Room
(The amber room is located on the second floor above the North American Museum of Ancient Life)
Pricing: \$250 for ISACA members
\$300 for non-ISACA members
*Member prices are also given to ISSA, IIA, and Students
Register: Go to <http://www.isaca-ut.org/utaevents.html> and follow instructions

Speaker Bio:

Steven F. Fox has over 18 years experience consulting for educational institutions, nonprofit organizations, Big Three Motor Companies, and training providers. He is a published author and speaker addressing information security within the enterprise. He is the principal consultant and founder of secureLexicon LLC, a company specializing in vulnerability and risk analysis. He serves on the board of the Detroit ISSA chapter and works closely with the SE Michigan Information Security Regional Skills Alliance. Mr. Fox holds a Masters in Business Information Technology from Walsh College; an NSA designated Center of Excellence.

Learning Objectives:

- Learn how develop and implement an organizational risk assessment process
- Analyze the process of the enterprise
- Understand the Unified Modeling Language
- Learn to discern risks from vulnerabilities using use cases
- How to document risk in the context of business processes
- Learn to translate risk-relevant use cases into risk cases
- How to think like the stakeholders

(Details of seminar topics see next page)

Overview of Seminar Topics

UML Primer

Notation overview
Modeling processes with UML

Risk Assessment Methodology

Getting started

- Pre-vulnerability assessment research
- What kind of business is it?
- What is the technical environment?
- How to construct a profile of the client company.
- Includes all information gathered during research

Get to know the business.

- Schedule interviews with stakeholders
- Create use cases to model business processes
- Use cases will illustrate the interaction of personnel and processes with assets within the enterprise.

What can go wrong?

Performing a vulnerability assessment

- Leveraging use cases to detect and model vulnerabilities.
- Review of tools that expose vulnerabilities.
- Mapping vulnerabilities to business processes.
- Given interconnected processes and technology within the enterprise, few vulnerabilities are limited to a single component of the system.

What matters to the business?

The Business Impact Analysis

- Review vulnerabilities for their impact on the business
- Assigning a risk metric and discerning risks from the vulnerabilities discovered earlier in the process
- Create risk cases that show the risk agent interacting with the relevant asset or process discussed in the case
- Determine the cost of an incident

How do we manage the risks?

- Leverage documents produced in previous activities to determine what controls make sense to the business
- Controls currently in place
- Selecting new controls
- Cost Benefit Analysis

Presenting findings and recommendations