Panel: Alternative Assurance: There's Gotta Be a Better Way!

Abstract: Traditional methods for ensuring that policies are enforced by Information Technology have proven slow and ill-matched for many of today's needs. This panel is designed to highlight the events at the June '96 Workshop on Information Technology Assurance and Trustworthiness (WITAT '96) towards evolving practical solutions for business and industry in need of confidence in their information systems. This panel will explore the available alternative assurance approaches and discuss their use for today's expanded and demanding assurance needs. Areas of assurance explored include, assurance predictors, system analysis and operational assurance, and impact mitigation.

Douglas J. Landoll

Arca Systems, Inc.

(703) 734-5611

(703) 790-0385 Fax

landoll@arca.com

ALTERNATIVE ASSURANCE: THERE'S GOTTA BE A BETTER WAY!

This panel is designed to highlight the events at the Workshop on Information Technology Assurance and Trustworthiness (WITAT '96), held on Sept. 3- 5, 1996. This workshop is intended as an initial step towards evolving practical solutions for business and industry in need of confidence in their information systems. The focus of this year's WITAT is to determine the merits of alternative assurance approaches and to create a strategy for developing the promising areas. Issues about these alternative assurances will be discussed between audience members and panelists. Additionally, results of the workshop and plans for developing promising assurance methods will be presented. The panelists are industry experts who will be chosen as subgroup chairs during WITAT '96.

WITAT '96 - In 1994, the Aerospace Computer Security Associates (ACSA) and the National Institute of Standards and Technology, responding to a perceived growing need in the community, organized and sponsored the Invitational Workshop on Information Technology Assurance and Trustworthiness (IWITAT). The success of this workshop led to WITAT '95 and now the planning for WITAT '96.

PANEL DESCRIPTION

Panel Introduction (10 minutes)

Doug Landoll (WITAT '96 Chairman) Arca Systems, Inc.

Traditional methods for ensuring that policies are enforced by Information Technology have proven slow and ill-matched for many of today's needs. This panelist will establish a framework for the remainder of the panel to explore the available alternative assurance approaches and discuss their use for today's expanded and demanding assurance needs.

Assurance Predictors (20 min. -15 presentation, 5 questions)
Mr. John J. Adams, NSA

Mr. Adams has focused his work at NSA for the past 3 years on alternative assurance methods. Two projects of note are the SSE-CMM and the TCMM. He participated in WITAT '96 and will report on the results of the workshop's discussion on Assurance Predictors.

Can assurance in an information system be gained from looking at the capability of the organization or individuals involved in develop/integrating/maintaining/operating the system? There are many methods that provide information about organizational or individual capability. What assurance do these methods provide?

WITAT '96 discussed various methods that indicate an organization's or individual's capabilities in an attempt to answer the above questions. The methods to be discussed include:
Capability Maturity Models (CMMs), the Generally Accepted System Security Practices (GSSP), International Information System Security Certification Consortium (ISC2), ISO 9000 series, Past Performance and Trusted Software Development Methodology (TSDM).

System Analysis & Operational Assurance (20 min. - 15 presentation, 5 questions)

(System Analysis & Operational Assurance Subgroup Chair)

System Analysis: The most direct way to achieve assurance in an information system is to analyze it directly. This panelist will discuss traditional authoritative methods such as TPEP and ITSEM and the acceptance of less authoritative independent testing.

Operational Assurance: Product and system assurance is only one ingredient involved in gaining confidence in an operation. Operational assurance depends not only on the information technology, but also on the people, environment, and processes involved. Even if information technology was 100% free of flaws, people would have to install, configure, and use it correctly to be secure. A panel will discuss the available methods for gaining operational assurance. The methods studied included: setting policy, risk assessment, background checks, configuration management, training, monitoring, and incident response.

Impact Mitigation (20 min. -15 presentation, 5 questions)

(Impact Mitigation Subgroup Chair)

Other known assurance techniques focus on reducing the vulnerabilities of the information system. These new types of assurance are not related to avoiding vulnerabilities of the system at all, but instead seek to mitigate the impact of defects usually in the form of software fixes or monetary reimbursement. This panelist will discuss several impact reduction assurance methods including warrantees, insurance, and legal liability.

Determining the Appropriate Mix (20 min. -15 presentation, 5 questions)

(Determining Assurance Mix Subgroup Chair)

What is the right mix of assurance approaches for your organization? This panelist will discuss the most effective combinations of assurance approaches for commercial and government systems, depending upon factors such as environment, reliance on technology, value of reputation, impact of security breaches, and connectivity needs. Different ways of composing assurance approaches will be presented including: assurance arguments, trade-offs, and criteria.