

# Information Assurance Posture Assessment Methodology

## Abstract

AverStar, Inc.

Shawn R. Campbell ([campbell@averstar.com](mailto:campbell@averstar.com))

George Linderborn ([glinderborn@averstar.com](mailto:glinderborn@averstar.com))

Ed Fuller ([efuller@averstar.com](mailto:efuller@averstar.com))

## Introduction

AverStar's Information Assurance Posture Assessment (IAPA) methodology focuses on the information, processes, and resources and uses vulnerability assessment (aka scanning) as a verification and validation mechanism of the findings of the assessment. This abstract describes the methodology, identifies the current, and projected activities associated with improvements of the methodology. Vulnerability assessments focused on systems and networks create environments where client resources are focused on correcting the effects not the cause of organization vulnerabilities. The IAPA's focus is determining the causes of vulnerabilities so that client resources can effectively and efficiently correct the causes, not the effects of the vulnerabilities.

## Background

The IAPA is a result of staff experience in the execution of Federal, Department of Defense, and Commercial risk assessment efforts, along with a correlation to industry assessment guidelines. The assessment guidelines that were used in developing the IAPA include: National Information Standards and Testing (NIST) Special Publications (SP) 800 series, Carnegie Mellon University Computer Emergency Response Team's OCTAVE, and the National Information Assurance Program's InfoSec Assessment Methodology.

The IAPA's cornerstones are the concepts of information sensitivity, process and resource criticality, and their critical path relationships. Sensitivity and criticality valuations are determined through close interactions between client organizations and the assessment team. The valuations are currently subjective in nature and structured similar to Mohs scale<sup>1</sup>.

Sensitive information categories are identified during those interactions and respective valuations of Confidentiality, Integrity, and Availability are linked with each category. Critical processes are identified and linked with respective information categories. Critical resources are identified and linked to the critical processes. Overlaying the sensitive information, critical processes, and critical resources on a topological technology view of the client organization's environment identifies critical paths. The critical paths are the primary focus of the vulnerability assessment. Information categories, Processes, and resources identified as having a low level of sensitivity or criticality are not scanned.

The assessment team uses the results of interviews, observation walkthroughs, industry research, documentation reviews, and vulnerability reports as input into a deficiency and gap analysis activity that results in a recommendation roadmap for the client. The roadmap is a Statement of Work for further mitigation implementation and planning activities. Subsequent risk analysis activities to determine the corrective actions are conducted during the mitigation implementation and planning efforts.

## Current and Projected Activities

Develop a distributed IAPA dashboard application that supports the IAPA activities. This application will be used to provide distributed access, concurrent management, a living repository, and dynamic risk management for clients, management, analysts, and the assessment team.

Research into valuation metrics. The research will focus on determining objective measurements of sensitivity and criticality.

---

<sup>1</sup> Derived from scale that was developed by Herr Mohs of Germany. The IAPA scale merely states that the higher numbered information category requires stronger controls than any lower numbered information category.