Security Assertions, Criteria, and Metrics Developed for the IRS

Paul Bicknell
The MITRE Corporation
Phone: (781) 271-3917 FAX: (718) 271-3957
Email: pab@mitre.org

Abstract

The Federal Information Technology Security Assessment Framework has been adopted by the Internal Revenue Service to provide a basis for conducting an evaluation of its cyber security program. The criteria contained in the framework have been expanded into security assertions, performance goals and metrics, and establish quantifiable security assessment targets. The goals and metrics are granular to the tasking level and allow for organization budget and tracking efforts.

Introduction

The Internal Revenue Service (IRS) is instituting a cyber security program based on the recognition of changing information processing technologies and threat environments. This has been brought about by the progressive replacement of old technologies such as mainframe processing with desktop/server environments and the recognition that the threats to information protection have become correspondingly complex. The introduction of new services such as electronic tax filing and the support of web servers and publicly accessible data resources are further necessitating the program.

The recognition of the evolving nature of threats prompted the IRS to search for a way to assess the condition of their current information technology protection program and to provide an improvement path. The IRS chose to utilize the Federal Information Technology Security Assessment Framework and to use its contents to develop security metrics that could be used to measure the current state of cyber security.

The Federal Information Technology Security Assessment Framework

In November 2000, the National Institute of Standards and Technology (NIST) released a document, titled: *Federal Information Technology Security Assessment Framework* (FITSAF), on behalf of the Federal Chief Information Officer Council. The express purpose of this document is to establish a foundation for organizations to use to measure the "state" of their cyber security programs. The framework adopted the concepts of a capability

maturity model and identified five levels of program effectiveness. The levels are: Document Security Policies; Document Security Procedures; Implement Policies and Procedures; Test and Review Implementation; and Fully Integrate Procedures and Controls. Criteria exist within each level, establishing the requirements that must be met by an organization in order for that organization's program to be considered compliant with the FITSAF.

Compliance with the FITSAF serves to provide assurances that an organization's information security program has established and implemented security policies, that responsibilities have been assigned and acknowledged, that necessary resources have been allocated, that risks have been addressed, and that security oversight is in place.

IRS Experience

The IRS adopted the FITSAF as the basis for establishing cyber security program goals. The initial effort focused on FITSAF Level 3 (i.e., Implement Policies and Procedures).

FITSAF criteria and requirements have been tailored to reflect specific IRS needs. The criteria were expanded into series of related security assertions. These assertions capture the elemental components of security within the criteria that must hold in order for the requirements to be met. This approach was taken so that a finely grained method for determining the condition of cyber security could be adopted. The assertions were further expanded into security performance goals and metrics.

Security Assertions, Performance Goals, and Metrics

The focus of the IRS's efforts in developing security metrics was to identify a quantifiable security assessment target based on the FITSAF Level 3 criteria. This was achieved by separating the FITSAF assessment criteria into 15 Security Categories, each pertaining to a specific portion of an effective cyber security program. The categories are: Security Policy and Planning, Risk Management, Review of Security Controls, Rules of Behavior, Life Cycle Management, Processing Authorization, Personnel, Physical and Environmental, Computer Support and Operations, Contingency Planning, Documentation, Training, Incident Response, Access Controls, and Audit Trails. Within these groupings, a baseline measurement capability was developed by introducing security metrics.

The 15 categories expand into separate criteria elements identifying individual Compliance Areas. The Compliance Areas relate to the activities performed to establish and verify the acceptability of a cyber security program. They provide a focus for the groups of goals and metrics. Security Assertions exist within each area.

The Security Assertions separate each Compliance Area statement into unique and fundamental components of security. They establish the conditions under which the Compliance Area (and therefore the criteria elements) will be met. They are composed of cyber security statements that will hold if the criteria are satisfied. They provide elemental objectives. Performance Criteria exist for each assertion.

The Performance Criteria establish the actions and results that are required to meet the assertion. They collectively represent the *things* that must happen or exist in order for the assertion to be valid. They are granular at the tasking level. This allows organizations to budget/track activities at this level. Further, an organization's progress towards FITSAF compliance is representable at this level.

Security Metrics exist for each Security Assertion and correspond to the Performance Criteria for that assertion. They represent the quantifiable measures of compliance. Three levels exist: non-compliance, partial compliance, and full compliance. Full compliance (or GREEN state) corresponds to having all the criteria met. Non-compliance (or RED state) corresponds to meeting few, if any, of the criteria. The YELLOW state (i.e., partial compliance) corresponds to meeting some identified subset of the criteria. For each assertion, some criteria are considered more vital for establishing a basis for meeting that assertion. Failure to meet these criteria could present a security mechanism implementation that served very little use and one that could be misleading in representing the state of the protections offered. These criteria constitute the set that must be met in order for any compliance to be recognized.

Security Metrics Example

The FITSAF contains requirements for System Auditing (at Levels 1 and 2) to develop policies and procedures for conducting auditing within an organization. This requirement states:

> FITSAF Requirement: An up-to-date security policy (at Level 1)/procedure (at Level 2) is written that covers audit trails.

The IRS adapted this requirement for its environment and introduced the Audit Trails Security Category. This category establishes a trackable grouping of all the relevant security requirements and metrics that are focused on audit trails. This includes audit trail creation, processing, and protection. This security category provides a shorthand method for consideration of auditing as a high-level security concept and allows auditing to be tracked (at this abstract level) as a singular element.

Within this security category a single Compliance Area exists. This Compliance Area represents Security Assertions at a high level and provides for the grouping of assertions into related subsets within a Security Category. For auditing, only a single, simple Compliance Area exists:

Compliance Area: Implement audit trail policies.

This Compliance Area is simple since the totality of audit considerations can be represented through a reference to the existence of audit trail policies. More complex Security Categories, such as Process Authorization, can have multiple Compliance Areas where the Security Assertions can be partitioned into multiple groups with similar focus. However, in this case a single area is sufficient.

For auditing, there are four Security Assertions within the Compliance Area. These assertions represent the four main policy elements for system auditing:

Assertion 1: The IRS has a formalized audit trail policy.

Assertion 2: Appropriate auditing capabilities are employed at both local and enterprise levels.

Assertion 3: A capability exists for audit analysis at both local and enterprise levels

Assertion 4: Audit trails are adequately protected.

These assertions together cover the elemental requirements for the existence of an effective organization-wide audit capability. At this level programmatic tracking of an overall effort to enact an audit program is possible, since the three primary elements of a program are identified. The elements are: audit records can be captured into audit trails, the capability to analyze the audit trails exists, and the audit trails can be preserved for later analysis.

Performance Criteria exist for each Security Assertion. These criteria establish the atomic elements that must be true in order for the Security Assertion to be met. In Assertion 2 above, for example, three criteria exist:

Performance Criteria 1: The assets requiring auditing at both local and enterprise levels are identified.

Performance Criteria 2: The type of information to be collected for each qualified asset is identified.

Performance Criteria 3: The duration for maintaining the audit trail at both local and enterprise levels for each system/application is specified.

Collectively, these criteria represent the essential capabilities that must exist in order for an audit mechanism to be found to be acceptable. Further, they can be used to establish separate tasking elements for the evaluation of an effective audit mechanism. Each of them can constitute a separate validation activity that can be accomplished independently.

Security Metrics exist for each Performance Criteria. These metrics provide a quantifiable measure against which each verification activity can be judged in order to determine if the essentials of each task have been accomplished. Three metrics exist for each Security Assertion, and this permits a red/yellow/green characterization of compliance assessment. The metrics for the three Performance Criteria of Assertion 2 are:

RED Metric: Either the assets requiring auditing are not identified, or no information is provided regarding what information is to be collected, or the length of time required to maintain the collected information is not specified.

YELLOW Metric: All assets requiring auditing are specified, but either the type of information to be collected or the length of time required to maintain the information is not specified.

GREEN Metric: All of the following is provided: assets requiring auditing are specified, the type of information to be collected is specified, and the duration for maintaining the collected information is specified.

For these metrics, based on the nature of the associated Performance Criteria, the RED (non-compliant) and GREEN (fully compliant) measurements are relatively simple. If none of the criteria are met, then the Assertion cannot be true and the metric is considered to be in the RED state. Likewise, if all of the criteria are met, then the assertion certainly holds and the metric is GREEN.

The YELLOW metric is more subjective if not all the criteria are met. A decision of relative significance is required to establish which criteria element is of primary importance in order for the assertion to be considered even partially met. In the case of auditing, the necessary criteria element is held to be the identification of all assets that require auditing. The other two criteria are considered to be lessor elements with a lower significance regarding the assurance of enacting an effective auditing capability. However, failure to identify the group of assets to provide auditing for, would result in an auditing system of essentially no value.

Conclusions

The FITSAF provides a federal government-wide means for assessing organizations' security programs. The IRS established a cyber security assessment program, adopted the FITSAF as the foundation of this program, and adapted the assessment framework to reflect IRS needs. Security Assertions, Performance Criteria, and Metrics were developed to provide a target for conducting cyber security assessments for this program.

These assertions, goals, and metrics provide for the programmatic tracking of compliance assessments. They establish a means to describe the current state of a cyber security effort and provide for the tracking of improvements to that program over time. Information for statistical analysis can be obtained from the use of these goals and metrics, and forecasting techniques can be used to manage programs over extended periods.

NOTE: This work would not have been possible without the IRS having a strong review process in place for checking compliance with security guidance and policy.