# PRISMA

Notes from

## Program Review for Information Security Management Assistance

**Author**: Davide Galassi

**Version**: 1.0.0
**Last Update**: 07-04-2018

# Table of Contents

# Acronyms and Keywords

| Keyword | Meaning |
|---|---|
| NIST | National Institute of Standards and Technology |
| ITL | (NIST) Information Technology Laboratory |
| FISMA | Federal Information Security Management Act (2002) |
| IS | Information Security |
| IG | Inspector General |
| CIP | Critical Infrastructure Protection |
| TA | Topic Area |
| FIPS | Federal Information Processing Standards |
| SEI | Software Engineering Institute |
| CMM | Capability Maturity Model |
| NSS | National Security System |
| CPIC | Capital Planning ad Investment Control |

# Introduction

In December 2002 the **E-Government Act** (Public Law 107-347) recognized the importance of information security for economic and national interests. The Law includes **FISMA**, the Federal Information Security Management Act.

FISMA charged **NIST ITL** to provide technical assistance to federal agencies regarding compliance with the standards and guidelines to protect **non-national security** related information.

Several sources of guidance, policies, standards and legislative acts provide many requirements for the federal agencies when protecting entrusted information. Various assessments, reviews, and evaluations are an outcome of these information security requirements to monitor federal agency compliance.

A standard approach to review and measure the posture of an organization with respect to the information security requirements is needed.

PRISMA is the framework developed and implemented by NIST to review the complex information security requirements and posture of a federal information security program.

PRISMA incorporates standards from the FIPS, guidance from many of the NIST Special Publications, existing federal directives including FISMA, and other proven techniques and recognized best practices in the area of information security.

The PRISMA methodology is a means of employing a standardized approach to review and measure the information security posture of an information security program.

PRISMA is not an Audit is an Assessment.

Possible objectives:

- Identify information security program deficiencies
- Establish a security program baseline to measure future improvement
- Validate completion of corrective actions
- Provide supporting information for the FISMA scorecard and report
- Prepare for or conduct an assessment, evaluation, or a review of an IS program
- Assist agencies in improving security of information and IT systems
- Help reduce disruption of critical federal operations and assets
- Improve CIP planning and implementation efforts
- Support the implementation of more systematic, risk-based, and cost-effective IS strategies.

FISMA assigned NIST the following responsabilities

- Developing IT standards for federal systems, to specifically include security standards and guidelines
- Conducting research to identify information security vulnerabilities and techniques to provide cost-effective information security
- Evaluating private-sector policies, practices, and commercially available technologies to assess potential application by agencies to strengthen information security
- Evaluating security policies and practices developed for NSS to assess potential application for non-national security systems

One of the outputs of a PRISMA review is a **maturity-based** scorecard focusing on nine primary **Topic Areas** of IS. This output provides a clear indication of the posture of the agency's IS program, which can then be used for executive decision-making.

**Audience**

- Management personnel with a role in Information Security
- Info Sec personnel
- Internal reviewers
- Auditors, both internal and external
- Inspector General staff personnel

# Approach Overview

A successful scalable process and approach to evaluating an organization’s IS program. Simply employing the methodical approaches increases the IS awareness of the agency personnel.

PRISMA review focuses on part or all of the strategic an technical aspects of an IS program.

## Topic Areas

The framework defines the following Topic Areas

- Information Security Management and Culture
- Information Security Planning
- Security Awareness, Training and Education
- Budget and Resources
- Life Cycle Management
- Certification and Accreditation
- Critical Infrastructure Protection
- Incident and Emergency Response
- Security Controls (Technical Aspects)

Each **TA** above consists of **Subtopic Areas** and each **STA** consists of a number of **TA Criteria**.

The maturity method is based on the SEI’s former **CMM** where an organization’s developmental advancement is measured with maturity levels.

## Maturity Levels

The framework defines the following maturity levels (in increasing maturity order):

- Policies : existence of documented IS policies.
- Procedures : existence of documented procedures developed from the policies.
- Implemented : review of the implementation of the policies and procedures.
- Tested : review the testing of the implemented policies and procedures.

- Integrated : review the integration of the integration of the previous maturity levels.

A higher maturity level can be attained only if the previous one is attained.

For example, if an agency has correctly implemented the policies, but no proper policy documentation exists then level 3 cannot be attained (nor 2 in this example).

For each maturity level follows a (not exhaustive) list with a description of the core points.

## Policies

- Formal, up-to-date, documented policies exist and are readily available to the employees.
- Written to cover all major facilities and operations agency-wide or for a specific asset.
- Approved by key affected parties.
- Identify specific penalties and disciplinary actions if policy is not followed.

## Procedures

- Formal, up-to-date, documented procedures are provided to implement the controls identified by the policies.
- Clarify *where, when*, *who* and on *what* and *how* a procedure is performed.
- Define expected behavior and responsibilities for asset owners/users, information resources management and IS administrators.
- Contains individuals to be contacted for further information

## Implementation

- Procedures are communicated to the individual that are required to follow them.
- Controls are implemented consistently everywhere the procedure applies and reinforced through training.
- *Ad-hoc* approaches are discouraged.
- Initial testing is performed.

## Test

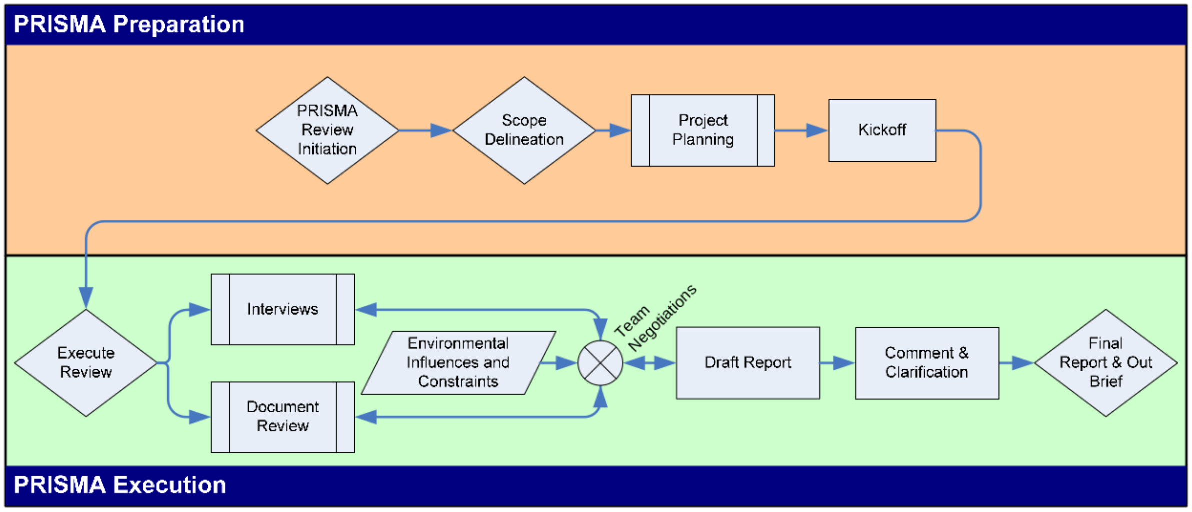
- Tests routinely conducted to evaluate the implementations.
- Ensure that all policies, procedures and controls are acting as intended.
- Corrective actions taken to address identified weaknesses.
- Self-assessments are routinely conducted.
- Information gained from records of potential and actual security incidents and alerts are considered test results.
- Frequency an rigor with which controls are tested depends on the risks if the controls are not operating correctly.

## Integration

- Policies, procedures, implementations and tests are continually reviewed and improved.
- A comprehensive IS program is part of the culture.
- Decision making is based on cost, risk and impact.
- Information Security is integrated into the CPIC.
- Security vulnerabilities are understood and managed.

# Review Steps

The review steps are graphically reported in the following image



# Preparation

## Review Initiation

Establishes the “need” for the review. May include: determine IS program gaps, ascertain program maturity levels, independent validation of program, audit or inspection demanded by higher authority.

A group of objectives are developed based on the “**need**”.

May include: identify deficiencies, establish baseline to measure future growth, justifying a continued budget support for a IS program, support information for FISMA scorecard, preparation for conducting an IG review.

Appropriate management level endorsement is crucial for appropriate usage of organizational resources.

## Scope Delineation

The review can be applied to only address subsets of the overall agency, program level, topic areas, maturity levels.

### Planning

Primarily concerned with resource and schedule planning.

Secondary primary and alternate key personnel is identified and notified, supporting documents are identified and cataloged.

Key IS representatives should compile a questionnaire to fine tune the review.

### Kickoff Meeting

A meeting between the party implementing PRISMA (auditors, inspectors) and the representatives of the IS program under review.

Identified objectives, scope, schedule, documents and related interview approach are briefed.

## Execution

### Documents Review

All the documents pertaining to each of the TA within the scope of the review and the maturity objectives are reviewed. A document can be "*compliant*", "*partially compliant*", or "*not compliant*".

Policy compliance can only be found in an organizational recognized policy document. Documents, especially policy and procedures, must be identified as "Final" and "Approved". Quality and quantity of documents must be considered. Every STA must be properly documented, otherwise a partial compliance is attained.

### Interviews

Provide information regarding personnel knowledge of information in the documentation and their attitudes. Two interviewers are suggested to avoid misunderstandings. The interviews are conducted minimizing the impact on daily personnel activities. Generally a 45/60 minutes interview is conducted.

Make introductions and explain the purpose of the PRISMA review and of the individual interview (i.e. identify strengths and weakness of IS program not obtainable from the docs).

There is non-attribution of the responses contained in the data stores and final report, even if applicability is dependent on the context. Anyway names are not recorded within the responses.

Ask only questions assigned to the interviewee position type. Eventually ask if the individual has suggestions of the IS program.

After the interview, both the interviewers document the results independently. Discrepancies are then resolved (maybe three interviewers are better) to produce a comprehensive interview document. The answer should be complete enough to make deduction of question obvious.

## Environmental Influences and Constraints

Identify positive and negative environmental influences and constraints bearing on the IS program. Examples: budget constraints, organizational cultural influences, organizational structures.

## Team Negotiations

Periodically through the review, review team members should meet to discuss progresses. In these phases some observations and recommendation can start to emerge.

## Data Analysis

Scoring process begins at the individual PRISMA criterion level where each document criterion has five maturity level questions (i.e. one to eval policy, one for procedures, one for implementation, ..).

For each criterion in a document review, the team members begin at the lowest maturity level to determine compliance. If all the results to a maturity question for a specific criterion for all documents reviewed are “Non compliant” the overall maturity level is scored “Non compliant”.

A non compliance at a maturity level imply non conformance to the higher maturity levels.

If at least one document is partially compliant, regarding a criterion question, then the overall maturity score for that criterion is considered “partially compliant” and the evaluation proceeds to the higher level criterion question (obviously there is a score).

Once the aggregation is completed across all document results for the TA criteria, the team aggregate the individual criteria scores into a summary for the STA and for the overall TA. The Criterion and STA are aggregated in the same fashion. For example a TA to be compliant all the STA should be compliant, if at least one STA is partially-compliant then the TA is partially compliant, in all the other cases the TA is non-compliant.

Once the aggregation is completed across all documents results for the TA criteria, the team must aggregate the individual criteria scores into a summary for the STA and for the overall TA.

For a specific maturity level, e.g. policy, if all the criterion maturity questions are non compliant then the STA policy is non compliant. If are all compliant then the STA is compliant. In all the other cases is partially compliant.

The aggregate score for the TA is generated in the same fashion.

In short, aggregation process consist in:

- Aggregate TA-criterion maturity level across all documents to produce TA-criterion evaluation.
- Aggregate TA-criterion evaluations to produce STA evaluation.
- Aggregate STA evaluations to produce TA evaluation.

Partial compliance is measured in scores between 0 and 1.

Further evaluation of upper maturity levels may be completed regardless of the PRISMA scores in order to support overall program recommendations, especially if one of the PRISMA Team's objectives is to estimate the resources needed to achieve a higher maturity level.

That is, the upper maturity level will be non compliant but a score can be given anyway!!!

## Issue and Corrective Action Identification

After the Review Team members aggregate scores, the information security issues are identified. The information is inferred from the scores of document review, environmental influences and constraints, and interview information.

Each issue statement is supported by a description of what was found that identified the issue.

Along with an issue statement and description, the team identify recommended corrective actions the organization can employ to resolve an issue. Associated with each action is an estimate of the time and resources to implement the action.

The review team prioritizes these actions according to the corrective action's **cost-benefit impact** on the maturity of the agency's information security program (e.g. with Pareto principle or the 80/20 rule: the 80% of effects comes from the 20% of the causes).

This prioritized list becomes the PRISMA report's **action plan**.

## Draft Report and Final Report

There is a recommended **template** for the Report: well defined **content and format**.

The information within the template can be modified to match the scope of the assessment, review or evaluation.

Sections:

- **Executive Summary**: max two pages containing a summary destinated to the stakeholders.

- **Background / Legislation**: background on IS and supporting legislation.
- **Review Activities**: an overview of the PRISMA process (documents reviewed and interviews coducted.
- **Review Observations**: positive and negative observations within separate subsections to each TA under the defined scope. This section should capture the TA related issues and subsequent recommendation(s).
- **Summary and FISMA Gap Analysis**: scorecards for each TA and their STA reviewed. Finally a FISMA gap analysis is developed from mapping PRISMA STA to FISMA requirements.
- **Recommended Action Plan**: in a prioritized fashion with a time schedule (short/medium/long term and if recurring).

### Report Review and Final Report

Appropriate management levels and **stakeholders** should be asked to review and comment on the draft report to **validate facts** and statements and to **evaluate the proposed corrective actions** and integrated **action plan**. PRISMA team should provide evidence to support the requested changes.

PRISMA Project manager and stakeholders make final decision on changes to incorporate. The final report is completed based upon acceptable changes.

## Applications

### Supporting Information for FISMA

PRISMA review researches, analyzes and provides information which directly respond to the FISMA report. The guidelines document provides a PRISMA to FISMA mapping table.

### Budged and Resources Justification

Supporting material for the agency CPIC, which is required to approve and prioritize all IT investments. Final Report recommendations based on a methodical approach, visual scorecards, and resource impact estimates can result in a strong argument for corrective action funding and approval.

### Information Security Awareness and Training

Information security personnel can visually see the information security program’s security posture and then learn about the criteria with partial or non-compliant scores.

When utilized in this manner PRISMA and the report are training tools to identify shortfalls and structure actions to improve security.

## Information Security Program Benchmark

The PRISMA Report not only provides a general overview of the information security program, but it can also provide very important results to dozens of information security criteria in an easy to understand visual presentation, effectively a security program benchmark.

This standardized format also provides the opportunity to “overlay” previous PRISMA reviews showing not only the current state of information security, but also the information security program’s maturation progress.

## Independent Validation of the “IS Program’s Security Posture”

With PRISMA’s library of criteria, an independent reviewer or evaluator may confirm the positive closure or mitigation of corrective actions. PRISMA provides a format which can easily present the security posture of the information security program in a customized presentation which is easily understandable by a broad range of technical and management backgrounds.

# Appendix: FIPS

Federal Information Processing Standards (FIPS) are **publicly** announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors.

FIPS standards are issued to establish requirements for various purposes such as ensuring computer security and interoperability, and are intended for cases in which suitable industry standards do not already exist.

Many FIPS specifications are modified versions of standards used in the technical communities, such as the American National Standards Institute (ANSI), International Standard Organization (ISO), International Electrical and Electronic Engineers (IEEE).