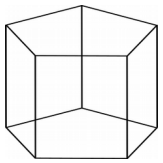


P R I S M A

Program **R**eview for **I**nformation **S**ecurity
Management **A**ssistance

Introduction

- In December 2002 the **E-Government Act** (Public Law 107-347) recognized the importance of information security for national economic and security interests.
- The E-Government Act 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.

Introduction

- Several sources of standards and legislative acts provide many requirements for the federal agencies when protecting entrusted information.
- Assessments, reviews, and evaluations are an outcome of these 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.

Introduction

- **PRISMA** is the **framework** developed and implemented by NIST to review the complex requirements of a federal IS program.
- Incorporates
  - standards from Federal Information Processing Standards (FIPS)
  - guidance from many of the NIST Special Publications
  - existing federal directives including FISMA
  - other proven techniques and recognized best practices in the area of information security.

Introduction

- The methodology is a **maturity based** approach to review and measure the information security posture of an information security program.
- The maturity method is based on the former Capability Maturity Model (**CMM**).
- Comes to help information security personnel, internal reviewers, auditors and the agency Inspector General.

Objectives

- **Identify** information security program **deficiencies**.
- Establish a security program baseline to **measure** future **improvements**.
- **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 information security program.
- Help **reduce disruption** of federal operations and **assets**.
- Support the implementation of a more **systematic**, **risk-based** and **cost effective** strategies.

Topic Areas

The maturity-based scorecard focus on **nine** primary **Topic Areas**

1) Information Security Management and Culture
2) Information Security Planning
3) Security Awareness, Training and Education
4) Budget and Resources
5) Life Cycle Management
6) Certification and Accreditation
7) Critical Infrastructure Protection
8) Incident and Emergency Response
9) Security Controls (Technical Aspects)

Each Topic Area (TA) consists of **Sub-Topic Areas** (STA) and each STA consists of a number of **TA criteria**.

Maturity levels

Maturity levels overview in increasing order.

- **Policies** : existence of documented IS policies.
- **Procedures** : existence of documented procedures developed from the policies.
- **Implementation** : policies and procedures implementation.
- **Testing** : policies and procedures implementation testing.
- **Integration** : continuous review and improvements are made.

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

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 the key affected parties.
- Identify specific penalties and disciplinary actions if the 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*, on *what* and *how* a procedure is performed.
- Define expected behavior and responsibilities for asset owners/users, information resources management and info sec 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.

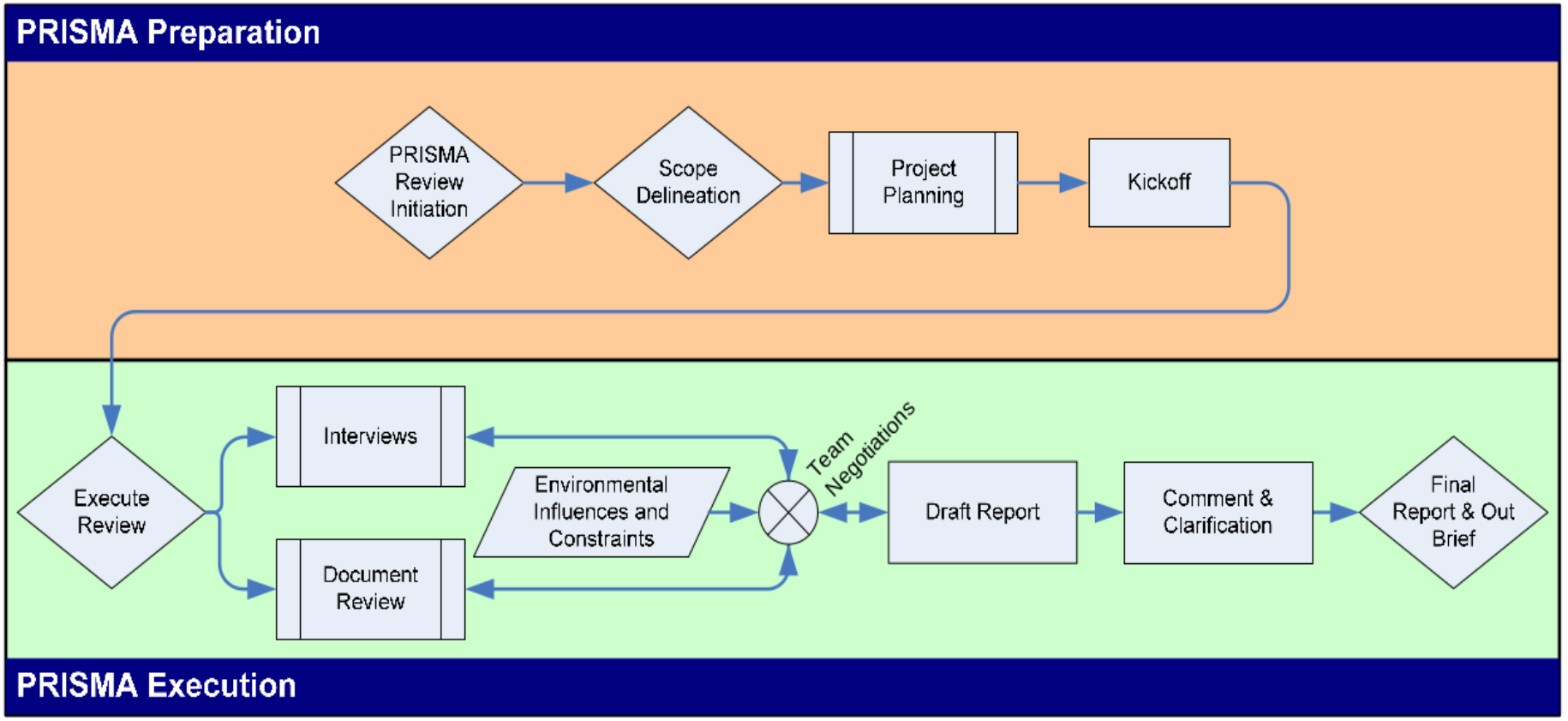
Testing

- Implementation tests are routinely conducted.
- Corrective actions taken to address identified weaknesses.
- Self-assessments are routinely conducted
- Information gained from records of (actual and potential) security incidents are test results.
- Frequency and rigor depends on the risks related to failures.

Integration

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

Review Steps



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.
- Tailored **objectives** are identified based on "*the need*" and the review **output** is identified.
- Appropriate management level **endorsement** is crucial for appropriate involvement of organizational resources.

Scope delineation

- The review can be applied to only address a **subset** of the overall agency, program level, topic areas and maturity levels.

- The appraisal is thus tailored and customized based on the required *need*.

Planning

Mainly concerned with resources and time schedule.

- Primary and alternate key personnel is identified and notified, supporting documents are identified and cataloged .
- Key information security representatives should compile a questionnaire to better fine tune the review.
- Care should be taken to don’t interfere too much with the personnel normal operations.

Kickoff meeting

- A meeting between the party implementing PRISMA (appraisal team) and the representatives of the information security program under review (stakeholders).
- Objectives, scope, schedule, documents and related interview approach are briefed and approved.
- The **Execution** phase begins

Document 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***".
- Documents, especially for policy and procedures, must be identified as "Final" and "Approved".
- Quality and quantity should be considered.
- Every STA must be properly documented, otherwise a partial compliance is attained.

Interviews

- Gather information regarding personnel knowledge of information in the documentation and their attitudes.
- The interviews are conducted minimizing the impact on daily personnel activities.
- No attribution of the responses, even if applicability is dependent on the context.
- Ask only questions assigned to the interviewee position type.
- The answer should be complete enough to make deduction of question obvious.

Environmental Influences

- Identify positive and negative environmental influences and constraints bearing on the information security program.

- Examples: budget constraints, organizational cultural influences, organizational structures.

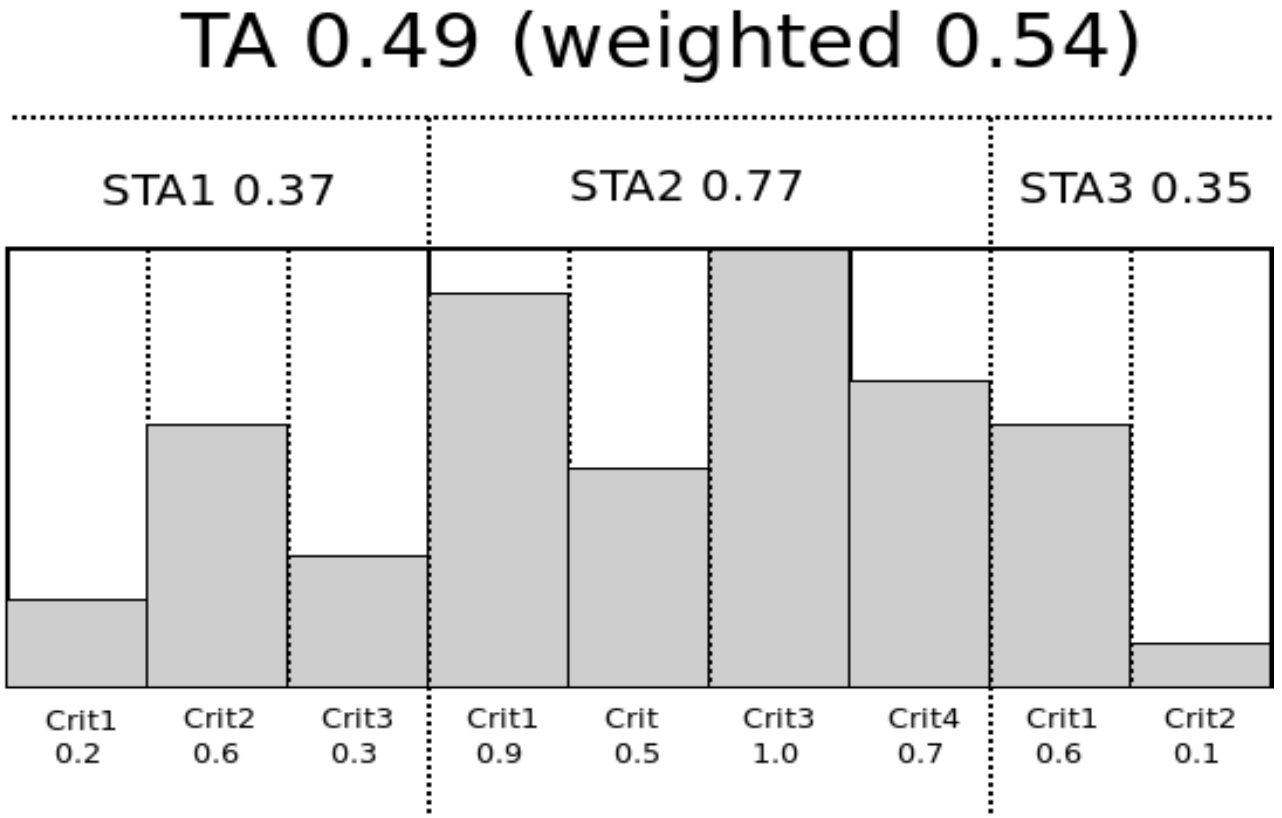
Data Analysis

- In a document review, for each criterion, the team members begin the evaluation from the lowest maturity level.
- If **ALL** the results to a maturity question for a specific criterion for all reviewed documents are "*non compliant*" the overall maturity level, for that criterion, is "*non compliant*"
- If **at least one** document is partially compliant to a criterion then the criterion is "*partially compliant*" and the evaluation proceeds to the higher level.
- For each TA criterion a score from 0 to 1 is computed by aggregating the single document scores.
- Non compliance at a maturity level implies non conformance to higher maturity levels.

Data Analysis

- Once the aggregation is completed across all documents for all the TA criteria, the team must aggregate the individual criteria scores into a summary for the STA and for the overall TA.
  - For each STA the scores are computed by aggregating the scores of each STA-criteria belonging to that STA.
  - For each TA the scores are computed by aggregating the scores of each STA scores belonging to that TA.
- Further evaluation of upper maturity levels may be completed regardless of the scores to support overall program recommendations
  - Especially if one of the objectives is to estimate the resources needed to achieve a higher maturity level.

Data Analysis



Is not clear if the TA and STA scores assignment should be weighted or not

Action Plan

- 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, recommended corrective actions are identified.
- Associated with each action is an estimate of the **time** and **resources** to implement the action.
- The actions are prioritized according to a **cost-benefit** impact (e.g. considering the Pareto principle or 80/20 rule)

Draft report

- A recommended template for the report is provided with a well defined content and format.
  - Simplifies inter-agency comparisons and contextualization.
  - Can be adapted to match the scope of the review.
- Template main sections:
  - **Executive Summary**: max two pages destinated to the stakeholders.
  - **Background / Legislation**: background on info sec and supporting legislation.
  - **Review Activities**: overview of the PRISMA process (docs reviewed and interviews).
  - **Observations**: positive and negative observations for each TA under analysis.
  - **Summary**: scorecards for each TA and their STA reviewed.
  - **FISMA Gap Analysis**: mapping of PRISMA STA to FISMA requirements.
  - **Recommended Action Plan**: prioritized and with a time schedule

Review and Final Report

- Appropriate management levels and stakeholders should be asked to review and comment on the draft.
- Facts and statements are validated 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 on the final report based upon acceptable changes

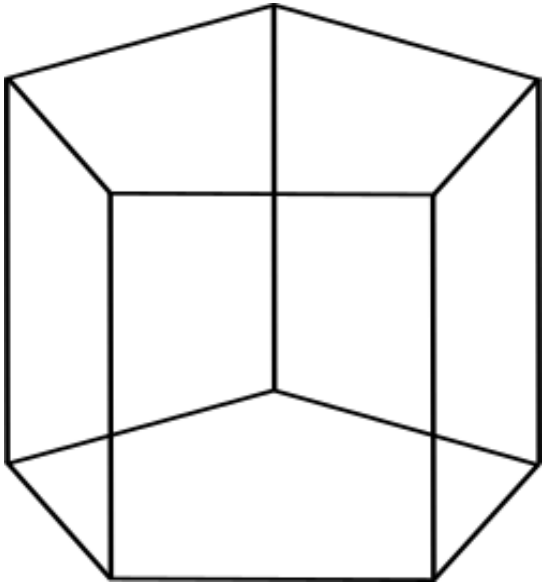
Applications

- Support Information for FISMA
- Budget and Resources Justification
- Information Security Awareness and Training
- Information Security Program Benchmark
- Independent Validation of the Info Sec program posture
- Review Preparation or Execution

Further information

- NIST public domain documents
  https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance
- Analysis notes
  https://datawok.net/files/2018/qc/prisma-notes.pdf
- Analysis slides
  https://datawok.net/files/2018/qc/prisma-present.pdf

T H A N K Y O U



Davide Galassi
davxy@datawok.net