- The Federal Financial Management Improvement Act (FFMIA) of 1996 requires accountability for financial results of actions taken.
- The Federal Managers Financial Integrity Act (FMFIA) of 1982 requires ongoing evaluations and reports on the adequacy of administrative control over internal accounting systems.
- The Clinger-Cohen Act of 1996 requires agencies to use a disciplined capital planning and investment control process to acquire and dispose IT resources.
- The E-Government Act of 2002 promotes better use of the Internet and other IT resources to improve government services.

Relevant OMB circulars and Homeland Security Directives

OMB Circular A-130 is known as Management of Federal Information Resources. Its appendix III titled Security of Federal Automated Information Resources deals with establishing a minimum set of controls to be included in federal automated information security programs, assigning federal agency responsibilities for the security of automated information, and linking agency automated information security programs and agency management control systems. The Homeland Security Presidential Directive 12 (HSPD-12), on the other hand, specifies a "policy for a common identification standard for all Federal employees and contractors." It aims to increase identification security and interoperability. It proposes to standardize the process of issuing a Federal employee or contractor an identification credential.

POAM

A plan of action and milestone POAM is sort of a corrective/remedial action plan that can be used to identify tasks that are to be accomplished. It states the resources that are required to accomplish the various plan elements as well as the milestones involved in meeting the tasks. This tool is especially useful for identifying, assessing, prioritizing, and monitoring the corrective efforts for the known security weaknesses. For this to work, all the security weaknesses that represent risk to the security of an IS program or IS system must be captured if planned mitigation is required.

You should have individual POAMs created for every program and system that has weaknesses identified. A program weakness may have the potential to impact multiple systems since there is a deficiency in the IS program. A system weakness is different - it is the result of a specific management, operational or technical control deficiency within an IS system. Each system weakness should be individually treated via a system-specific POAM.

It is necessary to prioritize the various POAM weaknesses due to resource limitations. Documented rank-ordering criteria can allow you to prioritize corrective actions in a standardized fashion against those factors specific to the operating environment in question.

Generally speaking, the POAMs prepared should be cross referenced to the budget materials of the corresponding agency (doing so can promote attention to security as a fundamental priority). Since the information in the POAMs is sensitive, agencies should submit or transmit POAMs using a secure method.

Review Questions:

1, COBIT is a standard intended for use by:

2, What is FISMA all about?

3, SoGP is a standard maintained by:

4, What is the focus of Val IT?