FISMA REPORT (federal information systems management act)

Meaning of FISMA REPORT

FISMA is a U.S. government legislation that defines a comprehensive framework to protect government information, operations, and assets against threats. Signed into law in 2002 and updated in 2014, FISMA requires that federal systems meet a set level of security requirements (also known as “controls”).

There are a handful of high-level requirements that can be summarized as follows:

1.maintain an inventory IT systems.
2.Categorize data and systems according to risk level.
3.Maintain a system security plan.
4.Utilize security controls.
5.Conduct risk assessments.
6.Certification and accreditation.
7.Conduct continuous monitoring.

Most efficient way is to consider the force-amplifying effects of automation.

Consider a tool ,or set of tools, that can pride the following capabilities to help significantly ease the time required for compliovance efforts and automatically:

Discover network devices and get an inventory of systems.
.Validate that devices have been correctly configured from a security standpoint.
.Validate that system and security patches have been applied across your systems.
.Monitor system logs to help identify threats or any malicious behavior.
.Block or quarantine malicious and suspicious activity.
.Monitor the system’s performance to catch failures as they begin to occur, and not after the failure leads to downtime.