An Introduction to Managing Compliance

Sateesh S Kannegala, Chief Consultant, Technology Management SecPod
sateeshks@secpod.com

Complex IT systems and their interactions are the reality of today's business world. For an organisation to function efficiently it is important to have security controls to ensure protection of confidentiality, integrity and availability of information and systems. Formulating the necessary security controls and adhering to the controls are essential to ensuring a secure system.

A weak server or an end point system is an easy target for attacks. Once compromised this system can become the conduit for data leakage and a source for unauthorized access of all systems in the network, wreaking untold damage on the enterprise. Implementing strict security controls, as determined appropriate by business and monitoring their effectiveness are critical to a smooth running business.

In this article we will address the process of compliance – the need for automation and how SecPod Saner provides enterprises the ability to automate the process of compliance and minimise the time spent in a noncompliant state.

Compliance

Compliance is the process of ensuring that all systems in an organisation meet a set of specified rules (system properties, configuration parameters, processes, etc.). The rules are determined as a part of a) Risk Mitigation strategy b) meeting industry standards for the business or c) meeting regulatory prescription.

A vulnerable system connected to the organisational network is a potential threat to the entire organisation (http://www.secpod.com/resource/whitepapers/Vulenrability-Malware-and-Risk-v1-1.2.pdf). A freshly installed OS is not usually configured with security in mind. Each Operating System comes with a set of guidelines – OS hardening guidelines. These guidelines plug loopholes that provide potential entry points used by attackers to gain unauthorised access to systems. Typical OS hardening measures include maintaining the system in a configuration where unnecessary services are stopped, blocking open ports, ensuring strong passwords, etc.

Many industry verticals have standards gleaned from years of experience. They are often presented as industry standards and they help optimize business performance. Industry standards have evolved to make sure businesses follow a set of rules designed to ensure fairness and security. Complying with industry standards provides customers a means of assessing the trustworthiness of the services provided by the vendor and to boost the confidence in doing business with them. Rules stemming from compliance requirements translate into specific needs on IT systems that support businesses.

Compliance Process

Figure 1 shows the process of compliance at a high level as suggested by ISO 27001. Compliance begins with a thorough evaluation of perceived risks to IT systems. Organisations spend considerable effort to define security policies, keeping in mind the nature of the business and the potential risk faced by the organisation. Security policies are comprehensive sets of rules to mitigate perceived risks faced by the business. Security policies also include controls resulting from regulatory requirements as well as applicable industry standards. For a security policy to be effective, it is critically important that all systems in the organisation comply with the policy set forth by the organisation.

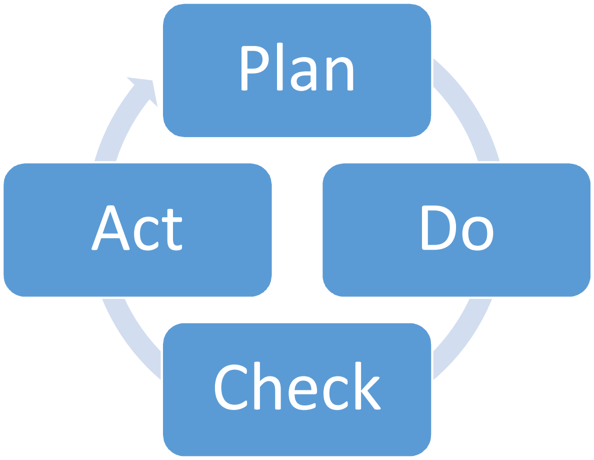

Figure 1

Once controls are established they are implemented in every system in the organisation.

It is well known that increased security is perceived as an inconvenience by users. A simple example of this would be the requirement of complex password rules. Remembering a complex password is difficult. Yet good security requires complex passwords. There can be additional requirements, such as, frequent changes to passwords and not allowing previously used passwords. All these make setting passwords even more difficult. Such inconveniences breed a tendency in people to try and circumvent security measures in the organisation – thereby increasing the risk to business.

In order to ensure IT systems are protected constantly, it is necessary to continuously check adherence to the policies set by the organisation. New vulnerabilities are discovered in software almost every day. These vulnerabilities provide entry points to attackers, thereby acting as a conduit to compromising the enterprise. Identifying and eliminating critical vulnerabilities becomes part of ensuring a robust safe environment. By establishing an organisational policy to check and remediate any known vulnerability, risk of attacks is considerably reduced.

Given the large number of systems in an organisation, ensuring continued compliance to policies becomes almost impossible unless the process of compliance is automated. Internal audits are conducted to provide reports of conformance to management. External audits are often required by regulation. The burden of proof during an external audit is on the organisation.

The security posture of an enterprise is not static. Over a period of time, the risks and the controls need to be re-evaluated and appropriate changes made to the policies.

From the foregoing discussion it is clear that accomplishing compliance is a daunting task. With thousands of systems in an organisation, ensuring that each system is compliant with either organisational policies or with regulatory requirements cannot be done manually.

Security Content Automation Protocol

The need for automation in evaluating and maintaining a good security posture requires organisations to use multiple tools. In the absence of a standard, organisations are forced to depend on proprietary data bases, data formats and scripts. Such an approach usually suffers from many drawbacks. Mostly key word driven, they are prone to errors and end up getting locked into proprietary data formats for each tool. They quickly become difficult to extend and almost impossible for an IT administrator to add or modify policies. The large number of systems and their variety makes it impossible to effectively manage compliance without standardisation.

SCAP – Security Content Automation Protocol was developed by NIST with the purpose of auditing security settings in workstations. "The Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans." (http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf)

SCAP enables standardised vulnerability management, measurement of policy compliance. It provides for enumeration of vulnerabilities and a means to assess their severity. Further, SCAP enables creation of machine readable checklists and configuration information.

SCAP is comprised of CVE (Common Vulnerability and Exposures), CCE (Common Configuration Enumeration), CPE (Common Platform Enumeration), OVAL (Open Vulnerability Assessment Language), CVSS (Common Vulnerability Scoring System) and XCCDF (eXtensible Configuration Checklist Description Format). These open standards help in automating Vulnerability Management, Configuration Management, Asset Management and Compliance Management.

CVE is a collection of over 69000 vulnerabilities and exposures and growing every day. CVE consists of a standard description for each vulnerability. This makes it possible for an organisation to use any CVE compatible source to get information about the problem. CVE allows users to choose any CVE compatible source for getting information on fixing the vulnerability. In addition, CVSS provides a convenient method to assess the criticality of each vulnerability. OVAL provides a standard for three steps of an assessment program, namely, representing the configuration information for testing, analysing the system and reporting. OVAL can be used for activities such as, vulnerability assessment, patch management, configuration management, asset management and auditing.

XCCDF is an XML specification for expressing benchmarks and evaluating results against the benchmark. XCCDF can be used to generate human readable reports and for building security checking tools. It is useful in automating compliance against known sets of rules. Some of the compelling advantages of XCCDF are: customise rules at run time; generate human readable reports in a standard format; compute and report rule status; easily integrate with any Information Security Management System.

Saner – An SCAP Compliant Product from SecPod

A secure IT system in an organisation requires the organisation develop a robust security policy and have the ability to implement and maintain the policy. While developing and customising organisational benchmarks is important to ensure minimal risk exposure, it is equally important to ensure adherence to the benchmarks.

Saner Business is a light-weight, enterprise grade endpoint vulnerability and risk management solution that provides comprehensive risk assessment, verifies compliance deviations and remediates issues to ensure endpoints are always protected and compliant. With an agent based architecture, Saner is capable of scanning thousands of systems in a very short time, ensuring virtually no downtime for the organisation. The agents access necessary security intelligence from a central repository, Ancor. Ancor is an exhaustive repository of well researched security intelligence along with tested patches for most known problems. Viser, with its rich reporting capability provides IT security managers visibility into the security status of all end point systems. Figure 2 shows a high-level schematic of Saner Business. Using Saner provides organisations the ability to scan all end points every day and remain compliant round the clock.

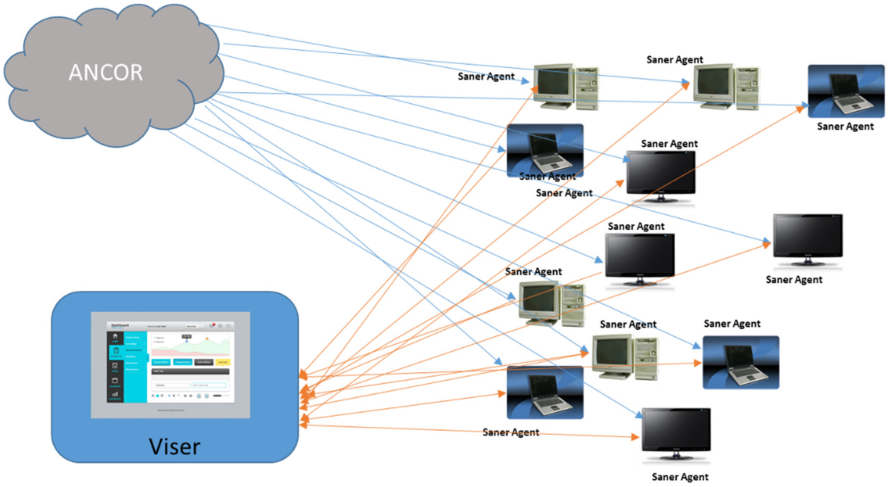

Figure 2 Schematic of Saner Business

SecPod Saner is a SCAP compliant product that helps organisations automate the compliance process. Consider for example, ISO 27001: the security process model of ISO 27001 is built around four areas: Plan, Do, Check and Act (PDCA). In the context of a modern enterprise, it is important to automate as many of these steps as practical.

Planning security requires an understanding of the context of the organisation and the risk exposure of the organisation. Using SCAP compliant reports generated by Saner, with scores associated with each vulnerability, IT security managers can get a quantitative estimate of exposure and implement measures commensurate with the risk.

With extensive checklists for various controls, including OS hardening and configurations from OS vendors, Saner makes it easy to create and customise security controls - thus implementing security controls is very intuitive.

The ability of Saner to remediate and rectify deviations from the checklist makes it very compelling. This ensures that any nonconformity can exist utmost between two scans of the system. Since scans happen every day, deviations are short lived. Because of this, the organisation always stays compliant with organisational policies and any regulatory standard that the organisation decides to follow. Without this ability IT managers have to manually look at the generated reports and act to remove discrepancies.

Saner, being SCAP compliant, easily integrates with any existing Information Security Management System (ISMS).

With simple interfaces and easy to read reports, Saner makes your organisation as invincible as you need it to be.