Who Gets Involved?

- The support of senior management is important to drive a VM program from the top down

- There are other participants whose roles should not be overlooked

- A clear definition of these roles can prevent
  - Considerable political strife
  - Streamline the development of process
  - Facilitate the deployment of technology, and
  - Encourage the assignment of individuals and groups to the VM effort

Who Gets Involved?

- **Contributing role** that helps the VM program get started and operate
- These participants are not directly involved in performing vulnerability assessments, but the process cannot proceed without their help
- Then, there is the **operational role**
- These participants are direct actors in the day-to-day operation of the VM technology
- They perform the scans, assess the vulnerabilities, and make sure that the priorities are raised to the right constituencies

Who Gets Involved?

- They also ensure that the VM technology continues to function optimally in a dynamic environment

- Some of the key groups involved in the VM process are
  - Asset Owners, Security, Human Resources, IT, Vulnerability Managers, Incident Managers, Change Management, and Compliance Management

- Each of these roles is either directly involved in the VM process or is at least affected significantly by it

Operational Roles

- Vulnerability Manager
  - This role is responsible for ensuring the correct configuration and operation of the technology
  - Also creating, monitoring, and distributing reports as needed
  - It is by no means a simple administrator role
  - The individual must be able to interpret technical reports produced by the system and to explain the cause and remediation for a Vulnerability
  - Knowledge of operating systems, networks, and security practices is required
  - This individual will interact with system administrators and network managers to ensure that the vulnerability identification and remediation processes meet goals

Operational Roles

- Incident Manager
  - When vulnerabilities require attention, one person must take responsibility for remediation
  - It is often the owner or administrator of the vulnerable target
  - This individual should have insight into the configuration and operation of the target and be able to assess the impact of a change to that system
  - This person, known as an incident manager, will work with the vulnerability manager to complete the required remediation tasks
  - It is the responsibility of the incident manager to follow up on the assigned remediation tasks until they are complete
  - In some cases, this role is combined with the role of change manager
  - For example, smaller organizations may have one person to field all work for engineers and administrators
  - This person could be responsible for receiving incidents, coordinating changes, and distributing remediation work

Operational Roles

- Change Manager
  - In a more complex remediation scenario where multiple systems or business functions may be affected by a complex change
  - The change manager will act as a project manager to oversee the full extent of the change
  - This manager will inform the affected parties, coordinate activities, perform testing or ensure that proper testing is completed
  - Work with the vulnerability manager to verify compliance

- Compliance Manager
  - This role is primarily one of a recipient and end user of the VM system and also one of the principal beneficiaries
  - In a normal compliance function, the compliance manager is tasked with ensuring that the systems in use by the company adhere to policies and standards

Operational Roles

- This manager is generally a recipient or consumer of reports from the VM system
- **The compliance manager will review trend reports to determine whether there is a continuous or repeating activity that results in a system being out of compliance**
- **This allows the compliance manager to discover processes in the organization that may be flawed in a way that leads to repeat policy deviations**
- In an environment where service level agreements (SLAs) are used to establish service levels
- The VM program manager may create an SLA for the compliance manager to ensure that audits take place at the required frequency and the appropriate checks are run on each target
- Metrics for this are simple and easily derived from the vulnerability scan results

Contributing Roles

- *Asset Owners*
  - Asset owners are those who ultimately pay for things and derive the most benefit
  - They control the purse strings and therefore have considerable say over what gets done
  - In many organizations, the asset owner is the line of business
  - Better cooperation in a large organization when making plans to assess the security posture of an asset
  - Two very important contributions of an asset owner are the
    - Asset classification and
    - valuation functions
  - Which cannot and should not be performed by the administrator of a system

Contributing Roles

- *Security*
  - Security departments are often the groups dealing directly with VM
  - However, organizations with a strong focus on service management, as described in the Information Technology Infrastructure Library (ITIL) service management framework
  - May consider this a subset of the existing framework
  - In either case, a close and cooperative relationship between the security function and IT should exist
  - A partnership will make VM implementation easier, and you will likely receive better internal support
- *HR*
  - One of the most overlooked groups
  - VM systems often find critical compliance problems, which can expand into evidence of security incidents perpetrated by an employee
  - HR is an instrumental part of the reporting process as well as the “stick” part of security policy

Contributing Roles

- HR is there to help manage the risk to the company from things that employees do
- HR is also involved in the creation and maintenance of performance management programs
- With careful planning, it is possible to tie vulnerability remediation performance to employee performance objectives
- To achieve this, it may be necessary to give HR a clear understanding of how the VM program and support systems work
- HR can then work with the VM program manager to determine what their role will be in mediating any potential conflicts that may arise with managing an employee

Contributing Roles

- *IT*
  - Information technology is obviously heavily involved in technology and process
  - A senior IT manager would also be very helpful in getting systems and networks remediated
  - The VM program manager should work with senior IT managers to develop the process and identify the key individuals who will oversee the work
  - In all likelihood, you will have to get some initial guidance from managers and then propose a process
  - Be sure to furnish a diagram
  - IT people work well with drawings and seem to commonly prefer analysing existing design