Program Structure

- Structure and composition of an IT or compliance organization can have a significant impact on the effectiveness of vulnerability management
- Understand the relationship between the business stakeholders and the managers of underlying IT assets
- If you can get the support of the business, then IT will be driven to support a VM program and comply with supporting policy
- VM must be a business priority, Otherwise, it is not worth doing
- VM Program encompasses all activities, technology, and personnel to specify, design, deploy, and operate the VM function
- Lays down the principles under which activities are conducted

Program Structure

- All activities, policies, procedures, and plans should be in furtherance of that charter, which functions like a constitution for the program
- It lays down the principles under which activities are conducted
- When questions arise about policy, procedures, or organization
- Charter can be consulted to determine whether decisions are being made in alignment with the business
- The charter is not a lengthy document with a lot of detail
- But rather a few carefully crafted sentences reflecting ethics, goals, and priorities of the company as they should be reflected in the VM function

Program Structure

- For example, if the company is intensely focused on availability of computing services because it is the primary generator of revenue
- Then a statement about not interfering with production computer operations should be included
- If the firm is more interested in the loss of confidential information
- Then a statement about identifying and remediating threats to confidentiality would be first
- **In the latter example, this would tend to place a higher priority on remediating vulnerabilities that might allow data to be stolen**

Program Structure

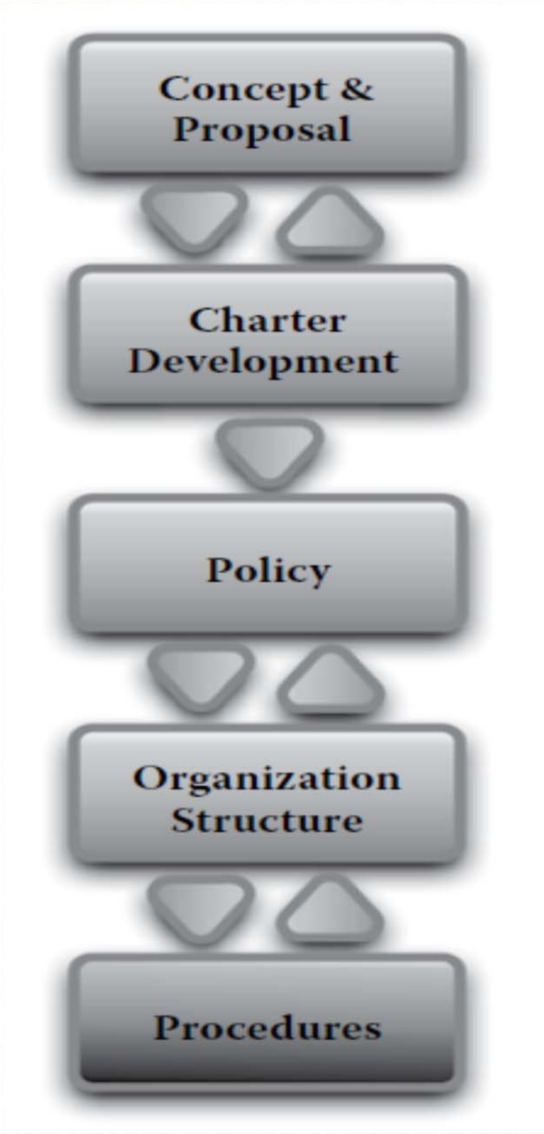
- During development of policies, procedures, and organization structure, new information is discovered that provides feedback into the overall program design

- That feedback loop may affect the organization structure or policies

- Figure in next slide illustrates the relationship among the program phases during the development cycle

Program Structure

- .



Program Structure

- Concept and proposal
  - Defines the business value that is to be provided to the business
  - The general concept of VM, and
  - At a high level, how one plans to achieve the results
  - This activity is primarily the responsibility of the program manager
- Charter development
  - The construction of a charter
  - These are the guiding principles and goals of the program
  - The charter is authored by the program manager and/or the executive sponsor

Program Structure

- Policy
  - Policies that support underlying business objectives, including any code of ethics that might exist
- Organization structure
  - An organization or combination of several organizations will fit together in a loosely coupled fashion to support the VM program
- Procedures
  - These are the detailed procedures that must be followed to support the VM program on a daily basis

The VM Program and Technology Development

- When the development of technology takes place in parallel with the organizational and procedural phases of the program
- Feedback must also inform upwardly, adjacently, and downwardly
- Adjacently, policy development may inform engineers on how to design a system
- Or, innovative design of the system may provide the ability to simplify procedures
- Downwardly, a subtle policy change may make coding of the system much simpler by removing an unnecessarily onerous internal audit capability

The VM Program and Technology Development

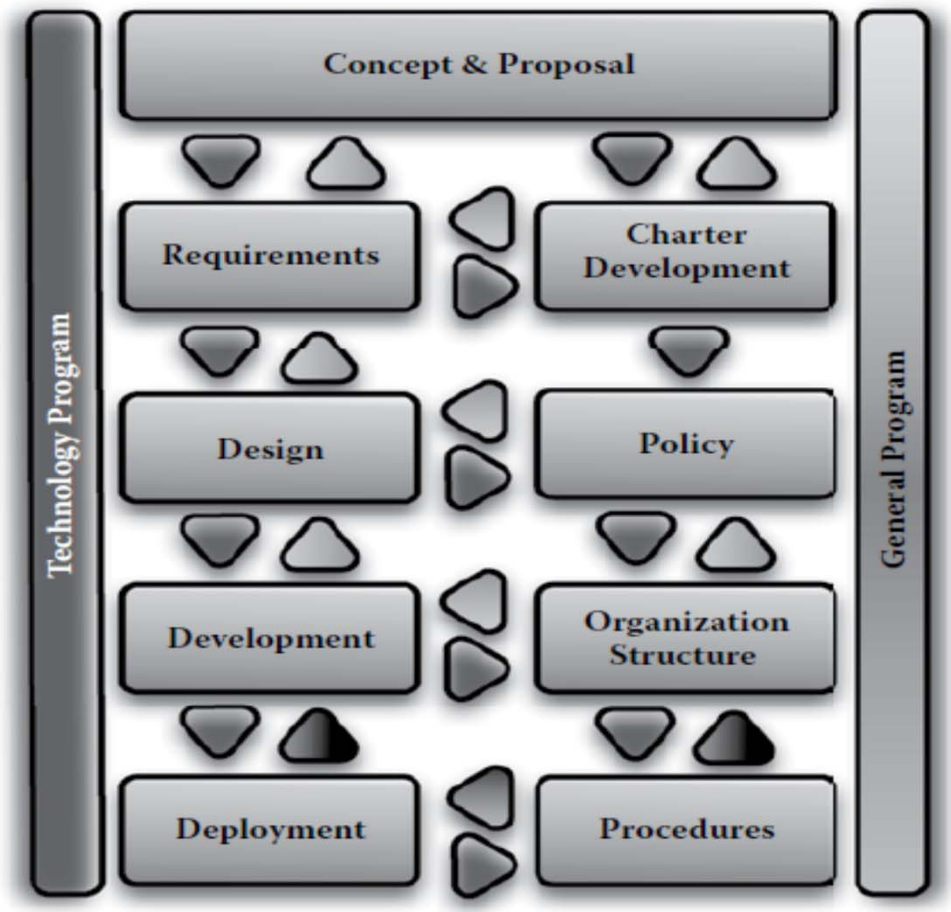
- A good example of this would be if the audit function required that every scan track each action taken by the system to detect vulnerabilities

- This would be an ill-informed policy because such recording activity would overwhelm any scanning software, hardware, or supporting network with audit information that would equal or exceed the actual vulnerability information discovered

- It would be more effective to consider the vulnerability result data as audit information itself

The VM Program and Technology Development

- .



e 3.2 Vulnerability management and parallel development process.

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