Rationale for a VM Program

- Why do we undertake a VM program? There are several good reasons, which are either technical or just make good business sense

- ***Overexposed Network***
  - Security Solutions not address all of the potential attacks from every vector
  - Not financially practical to put intrusion protection, antivirus, content filtering, traffic analysis, and application behaviour analysis on every single port on a network of 50,000 nodes
  - The only way to address these weaknesses is a basic defence-in-depth strategy that removes single points of failure
  - Most network security strategies rely on perimeter , if they fail, will leave a vulnerable host wide open to exploitation
  - This is overexposure at its worst

Rationale for a VM Program

- ***No Standard for Secure Systems Configuration***
  - Large companies typically develop one or more standard configurations for systems connected to a network
  - This includes standards for desktop and server operating systems, network devices, and even printer configurations. These standards often have security practices built in
  - When these standards are absent, more vulnerabilities are likely to exist than when the standards do not exist
  - Even if there is a patch management system in place, those configurations cannot be fully addressed by patches
  - In most cases, patch management systems will not find everything requiring remediation, It is no substitute for VM
  - The negative side of standardization is the ubiquity of vulnerabilities. If a standard configuration is deployed globally and has a vulnerability, then the vulnerability is everywhere

Rationale for a VM Program

- ***Risk of Major Revenue or Financial Loss***
  - When the risk of a breach is high, concerns of management naturally turn toward the impact of realizing the risk;
  - That is, with increasing regulation from government, the potential for financial loss greatly increases
  - These losses can come from litigation and/or civil penalties
  - Imagine losing a client's confidential data due to failure to remediate a critical, published vulnerability
  - When a client is lost, the business suffers not only the loss of revenue but also the damage to its reputation
  - It is ten times harder to recover from this than any other kind of loss
  - Businesses can do everyone a favour by being more diligent in managing vulnerabilities

Rationale for a VM Program

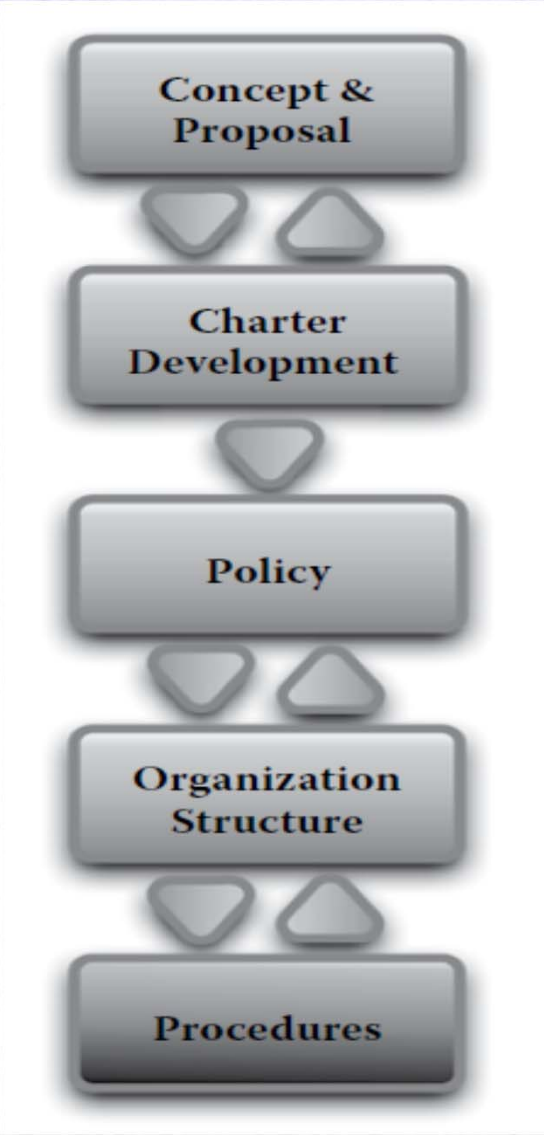
- ***Lost Productivity***
  - When systems are compromised, they often become unusable for a period of time
  - If these are critical systems, significant productivity is lost from employees who cannot perform their jobs
  - It is also often the case that many time-consuming activities must take place before a system is returned to service
  - The system must be analysed for the cause of the failure, rebuilt, patched, additional security considered, and closely monitored for a secondary attack

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
- 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

- .



Program Structure

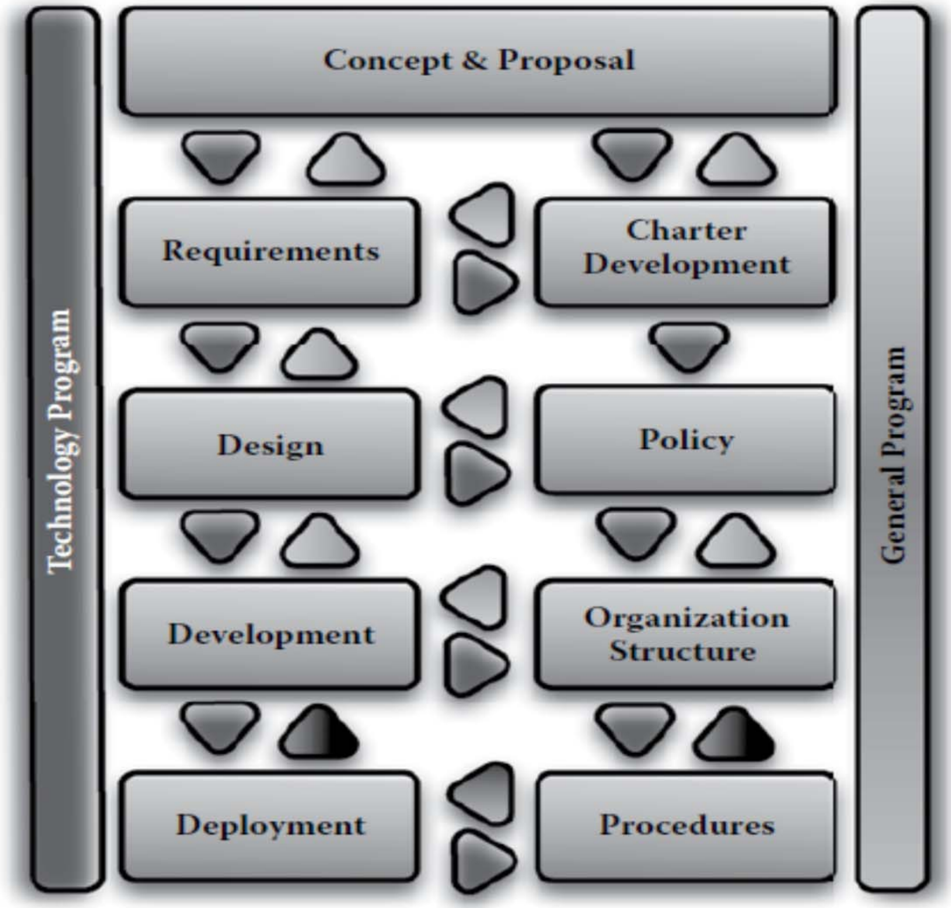
- Concept and proposal
  - Defines the business value that is to be provided to the business
  - The general concept of VM, and
  - At a high level, how one plans to achieve the results
  - This activity is primarily the responsibility of the program manager
- Charter development:
  - The construction 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

- .



e 3.2 **Vulnerability management and parallel development process.**