Bab XII. Manajemen *IT Policy Compliance*

Dr. Yeffry Handoko Putra

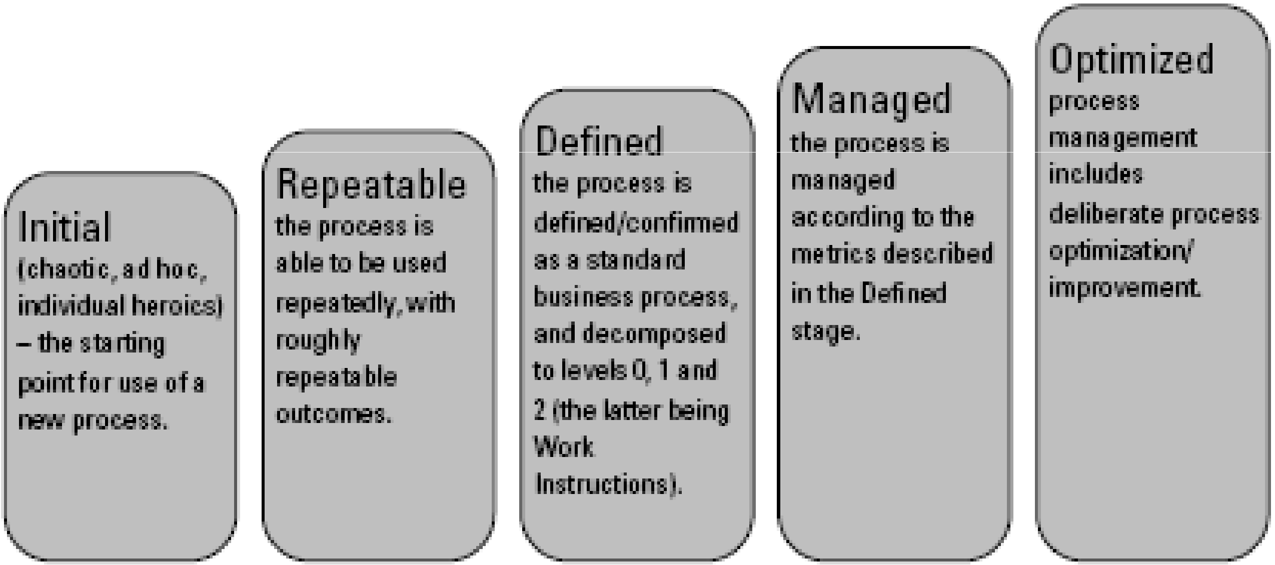
IT Policy Compliance Management

- Keeping a balanced perspective on IT policy compliance
- Understanding the auditor’s perspective
- Aligning IT compliance/security with business processes
- Building an IT compliance policy and controls environment
- Establishing and monitoring accountability
- Using risk-based prioritized remediation of control weaknesses

Remember the Big Picture

- ***Maintaining your perspective*** starts with understanding your organization’s policy control objectives
- **Understanding the auditor mentality**
- **What if fail?**
- **You have to prove it!**

Align IT Policy Compliance and Security with the Business



Initial
(chaotic, ad hoc, individual heroics) – the starting point for use of a new process.

Repeatable
the process is able to be used repeatedly, with roughly repeatable outcomes.

Defined
the process is defined/confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the latter being Work Instructions).

Managed
the process is managed according to the metrics described in the Defined stage.

Optimized
process management includes deliberate process optimization/ improvement.

Figure 3-1: The SEI Common Maturity Model.

Understand
Your Technology Environment

- **Identifying your environment:**
  - *homogeneous environment*
  - *Heterogeneous environments*
- **Bearing virtualization and cloud computing in mind**

  -- *Virtualization or the abstraction of IT resources is*

Understand
Your Technology Environment

- **Bearing virtualization and cloud computing in mind**
  -- *Virtualization or the abstraction of IT resources is*

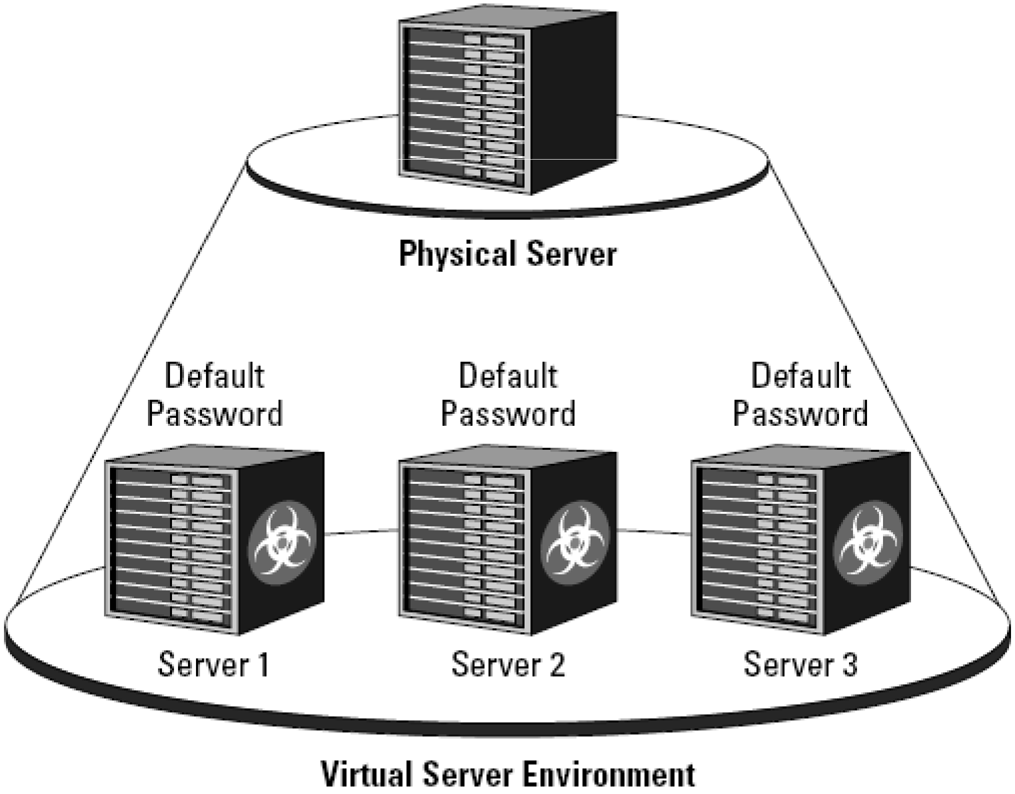
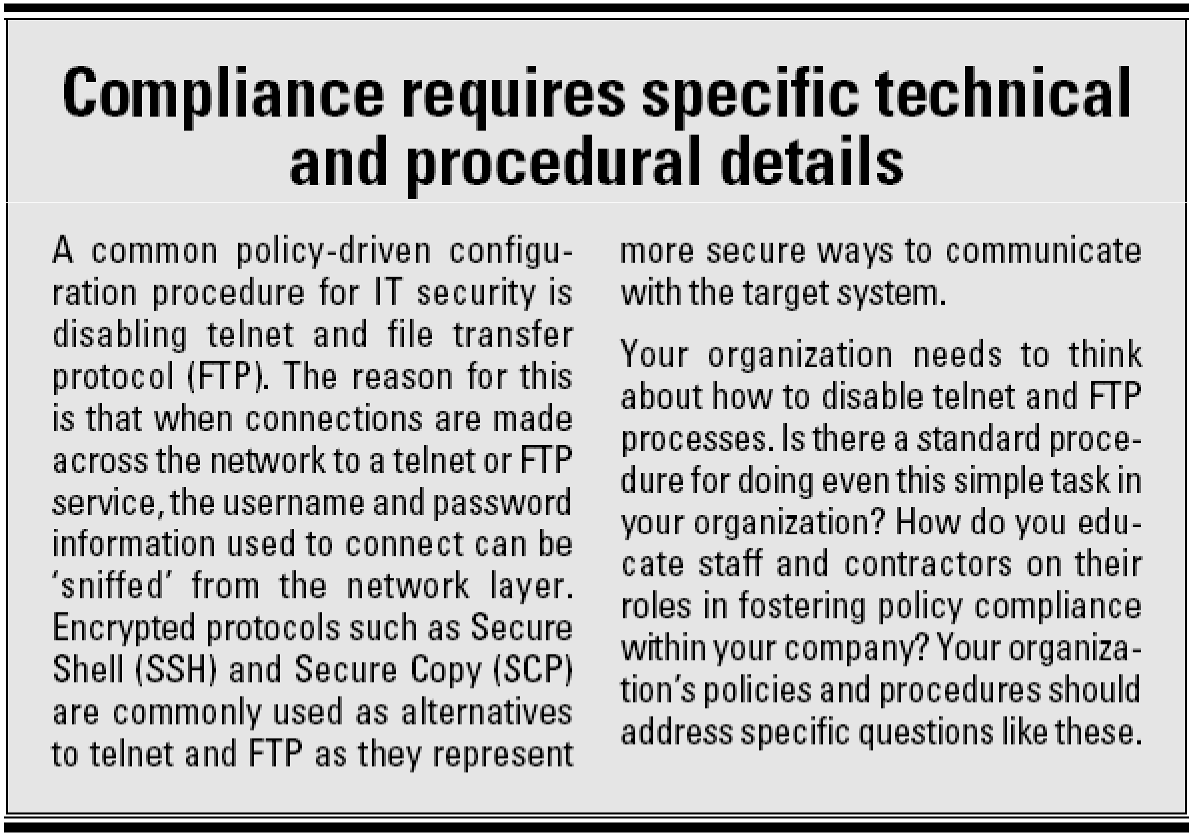


Figure 3-2: A single vulnerability is magnified in a virtualized environment.

IT Compliance Starts with Policy

- Compliance requires specific technical and procedural details



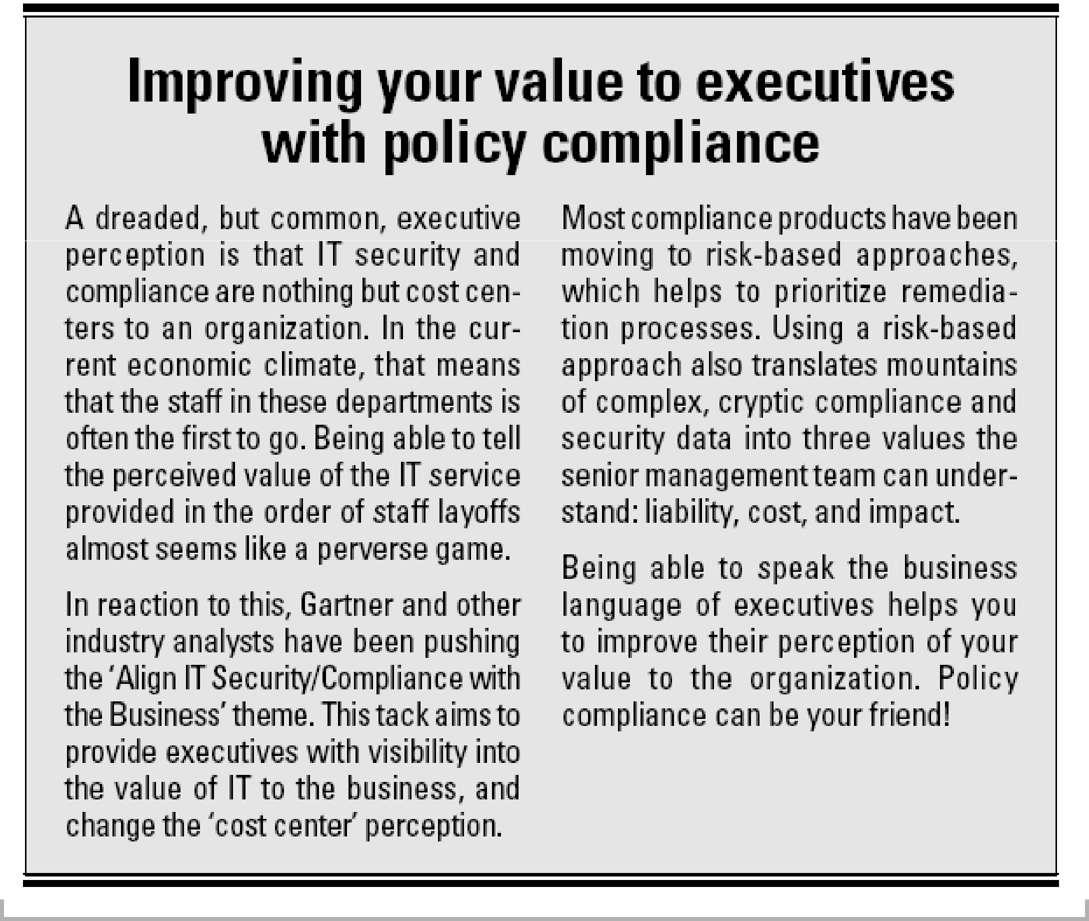
Compliance requires specific technical and procedural details

A common policy-driven configuration procedure for IT security is disabling telnet and file transfer protocol (FTP). The reason for this is that when connections are made across the network to a telnet or FTP service, the username and password information used to connect can be 'sniffed' from the network layer. Encrypted protocols such as Secure Shell (SSH) and Secure Copy (SCP) are commonly used as alternatives to telnet and FTP as they represent more secure ways to communicate with the target system.

Your organization needs to think about how to disable telnet and FTP processes. Is there a standard procedure for doing even this simple task in your organization? How do you educate staff and contractors on their roles in fostering policy compliance within your company? Your organization's policies and procedures should address specific questions like these.

Establish Accountability

- Starting at the top
- Defining roles and responsibilities
- Improving your value to executives with policy compliance



Improving your value to executives with policy compliance

A dreaded, but common, executive perception is that IT security and compliance are nothing but cost centers to an organization. In the current economic climate, that means that the staff in these departments is often the first to go. Being able to tell the perceived value of the IT service provided in the order of staff layoffs almost seems like a perverse game.

In reaction to this, Gartner and other industry analysts have been pushing the 'Align IT Security/Compliance with the Business' theme. This tack aims to provide executives with visibility into the value of IT to the business, and change the 'cost center' perception.

Most compliance products have been moving to risk-based approaches, which helps to prioritize remediation processes. Using a risk-based approach also translates mountains of complex, cryptic compliance and security data into three values the senior management team can understand: liability, cost, and impact.

Being able to speak the business language of executives helps you to improve their perception of your value to the organization. Policy compliance can be your friend!

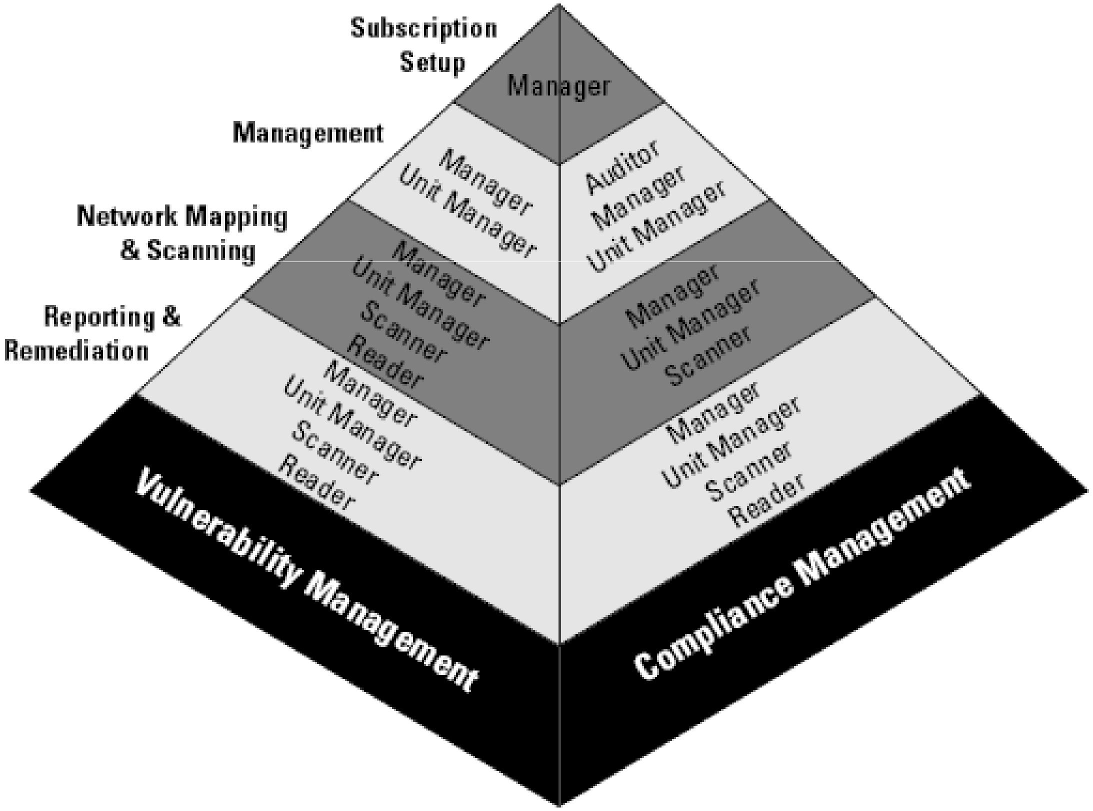


Figure 3-3: Roles and access permissions used with QualysGuard Policy Compliance.

Conduct a Pre-Audit or Readiness Assessment

- ✓ A policy and procedure review.
- ✓ An organizational review.
- ✓ A high-level controls architecture review.
- ✓ A review of previous audit reports.
- ✓ A comparison of a sample group of normal and administrative users' levels of access to what is necessary.
- ✓ A review of standard build documents.
- ✓ A comparison of a sample of systems with secure build documents.
- ✓ A review of change management procedures and selection of a sample of change tickets to review and see if procedures were followed.
- ✓ A review of incident-handling procedures and selection of a sample of tickets to review and see if procedures were followed.
- ✓ A physical and environmental control walk-through.

Centralize IT
Policy Program Management

- Select a common risk model and a set of standards for the organization.
- Normalize reporting so that values are consistent across regions and lines of business.
- Leverage a common set of industry standards such as CIS, AusCERT, ISO, or SANS.
- Validate that policies created by regional teams are accurate and applicable enterprise-wide.

A well-defined risk program includes common best practices

- Maintaining asset definitions and a process for keeping the inventory up to date, including business layer goals and objectives as part of an asset’s valuation.
- Understanding the threat landscape and how probability and consequence of threats are common pairings with vulnerabilities that top the list of remediation tasks.
- Conducting an ‘impact analysis’ of suggested changes to avoid negative effects of remediation activities on critical business processes.
- Implementing well-defined repeatable processes where a ‘rinse-lather-repeat’ cycle continuously improves and streamlines processes.
- Collaboration among regional teams to ensure components of the program are standardized and resource requirements are understood for all phases of the program.