

# Network Security Project Management Context and Process

Dr Zaheera Zainal Abidin



# Learning Objectives

- Understand the **CONTEXT** of how to manage projects involved with computer networks inside the organization and secure the network from cyber attacks or threats.
- Explain the **LIFE-CYCLE** of network security project management called as “**secure network life-cycle management**”.
- List important skills and attributes of **A GOOD PROJECT TEAM MANAGER**.
- Understand the **FOUR FRAMES** of organization.
- Understand the **PROCESS GROUP**.



The image features a hand holding a glowing blue network globe. The globe is composed of a complex web of blue lines and dots, representing a network. The background is dark blue with blurred server racks and glowing light effects. The text "MANAGEMENT OF NETWORK SECURITY PROJECTS CONTEXT" is overlaid on the image in a bold, sans-serif font. The words "MANAGEMENT OF" and "CONTEXT" are in yellow, while "NETWORK SECURITY PROJECTS" is in white.

# MANAGEMENT OF NETWORK SECURITY PROJECTS CONTEXT

# Network Security Project Management

## CONTEXT-1

- Managing the network security projects is a tedious and tantalizing process due to the evolution of threats and attacks.
- Projects are temporary but need to achieve the objective of the organization.
- Projects must operate in a holistic organization environment with a greater organizational context.
- The security approach is a critical method to obtain a successful project management.

# Network Security Project Management


## CONTEXT-2

- Several factors that project manager need to consider:
  - **Requirement and Scope**
    - A) Network architecture, B) Organization's Security Policy
  - **Technical Plan**
    - A) Project life cycle (deliverables and sequencing of deliverables), B) Activities to complete the deliverables
  - **Design Resources**
    - A) Talents and skills needed, B) Facilities required, C) Security tools needed
  - **Estimation**
    - security policy size (functionality), network size estimation, function point analysis, vector size measure, software security assurance and IT compliance in the network
  - **Project and security services risks**
    - A) Risk mitigation plan for the project; and for each process, assets and services

# Requirements and Scope

- The scope is influenced by the type and number of cyber attacks and threats; the organization's resources available; the desired response to an attack; and the network architecture or topology of the entire network system.
- A risk assessment should aid in identifying the highest priority threats and the profiles of the most point of likely attacked. Straightforward preventive measures may offer sufficient protection from the inexperienced attacker. Experienced and well-resourced external attackers and “insiders” require more elaborate tactics for protecting user data and privacy.

# Technical Plan

- The nature of threat and its consequences effects the cycle of the project development. The project activity with a low likelihood of risk, urged the project leader to decide. The management of high probability threats with medium level consequences would likely require external expert assistance and a well-defined systematic review process.
- Testing is influenced by risks. 
- A holistic risk analysis process provides an indirect measure of how well potential errors have been analyzed. There should be a close tie between the outcome of risk analysis and project requirements as risk analysis helps to define the scope for security in terms of threats to be considered, the response desired, and the assurance level required for that activity.



# Design Resources

- Talent requires a management for security level of services being produced, so that talent maps individual skills with services. Training and nurturing the skills of the talents is crucial.
- As assurance levels rise, the development process provide the necessary control and information protection mechanisms. Change management must be well controlled. High-assurance configuration management must support requirements for audit, traceability, and process enforcement.
- Security expertise on most projects is limited and may be an internal or a contracted service. The allocation of that resource is often difficult even when security activity is limited to networks, authentication, and access control, but when security has to be incorporated into application development, that expertise is spread much thinner. There may be specific tools required, such as for static code analysis, to aid the production or testing of secure software.



# Estimation

- The early identification is to estimate talents and assets available in the organization; potential attacks or threats; efforts or damage of processes and preventive costs on a large variance through the network size estimation and functionality at point of analysis.
- A vulnerability analysis model is developed with detailed attacker actions and possible responses in a detailed description of the security services provided in the proposed network architecture design.
- Shared infrastructure can reduce component development costs, but those shared services typically aggregate risks. Estimates should reflect the increased software security assurance that can be applied to the shared services.

# Project and Security Services Risks

- Poor management of requirements scope is another frequent cause for project failure. Scope management is important, since the immaturity of the business usage or the supporting technology depending on the identification process.
- Security mechanisms that mitigate a specific risk may create additional ones. For example, security requirements for managing identity for a large distributed system is obtained through implementing authentication and authorization as infrastructure services shared by all applications, but the aggregation of authentication and authorization mechanisms into a shared service makes that service a single point of failure and a possible attack target.



# How to protect the network? Some tips..

- **Backup Data Plan and Schedule**
- **Network Perimeter Protection**
  - Implement Routing Protocol – such as BGP and OSPF
  - Implement Switching Protocol – such as VLAN security, Access Lists Control
- **Network based Mitigation**
  - IDS/IPS to monitor incidents
  - Firewalls
  - Own the Emergency Response Team
- **Host based Mitigation**
  - https instead of http
  - Open port like 8080 has a timeout session
  - Host based Firewall
  - Update regularly the antivirus and antispyware
  - Always change passwords
  - Control the physical access at the network devices
- **Proactive Measures**
  - Neutralize the threat with programming codes develop by experts
- **Encryption on Backup Data**
- **Encryption on Authentication**
- **Conduct Audit and Risk Assessment**
  - Identify the Assets, Talents, Vulnerabilities, Potential Threat
  - Improve the Security Policy and Procedures
- **Restrict the Administrative Rights**
- **Implement VPN**
- **Awareness Program**
  - Teach employee on how to change password regularly and educate them for a strong password
  - Educate staff no to give HANDPHONE number, BANK ACCOUNT number and any private information to the hacker during the social engineering.
  - Do no panic if you have not do wrong. Just stop the conversation by putting down the phone.

# The Life-Cycle



# Secure Network Life-Cycle Management

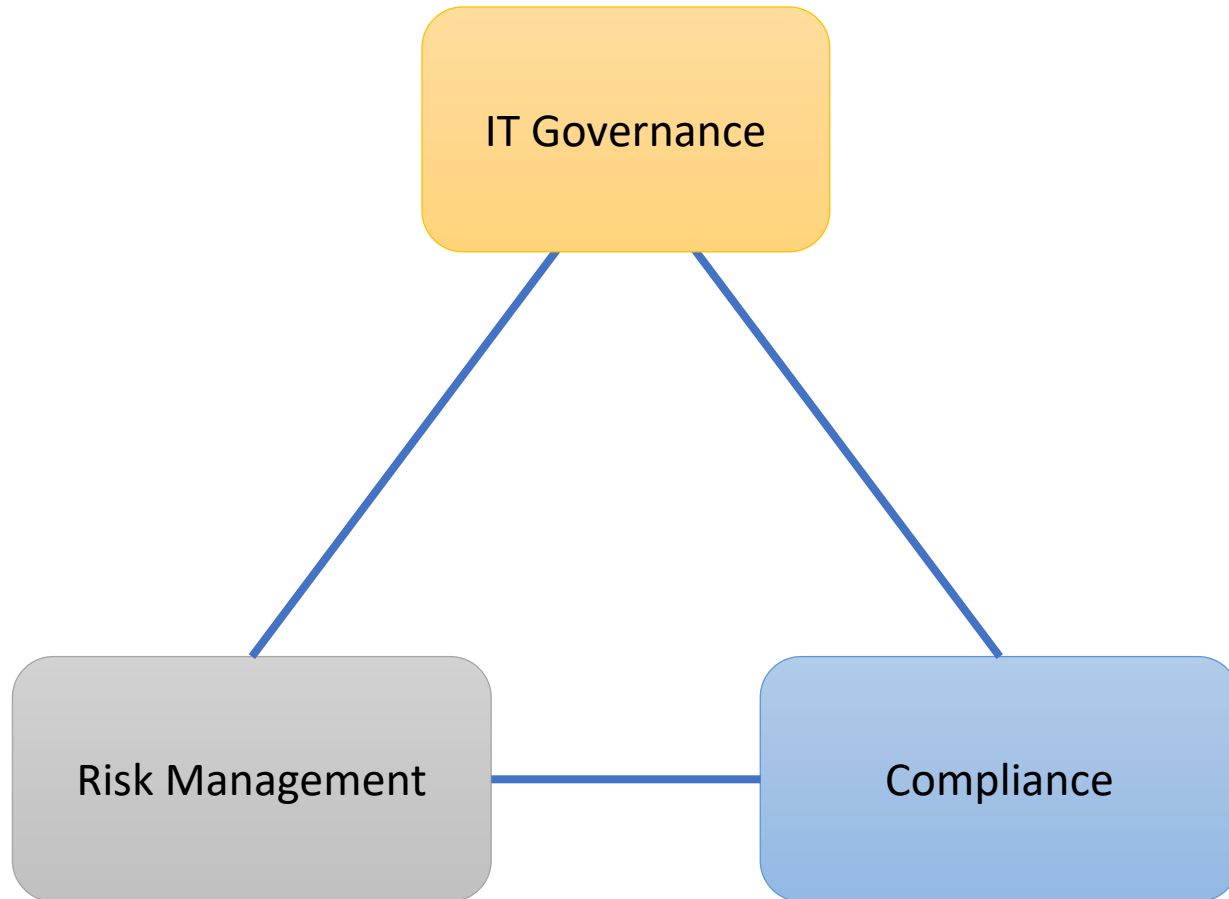
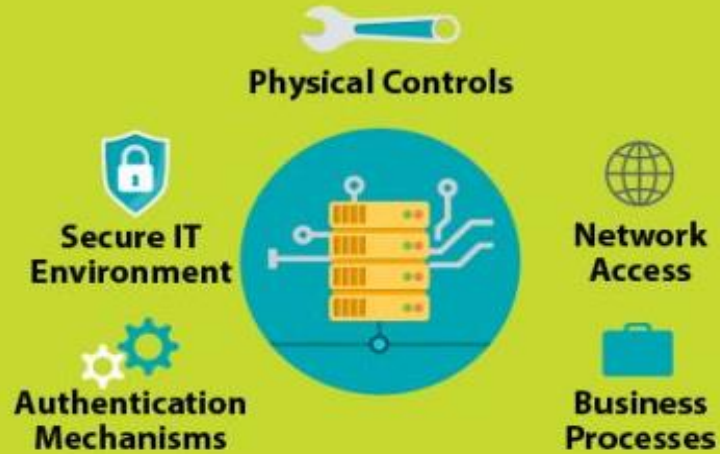


Figure 1: converged security policy

- According to CISCO, organization is governed under the integration of IT Governance, Risk Management and Compliance components.
- The aim is to :
  - avoid conflicts
  - avoid gaps,
  - avoid wasteful overlaps or redundancies.
  - improve the operational decision-making, strategic planning, and business value-added
  - IT security is part of the strategic initiative of the organization – either public or private.

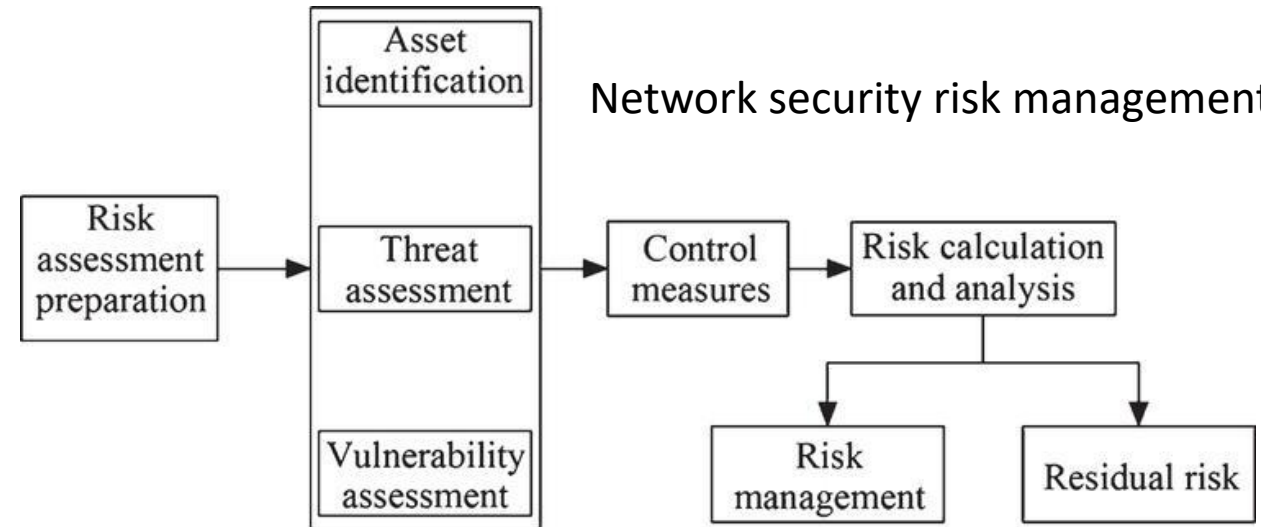
# SECURITY



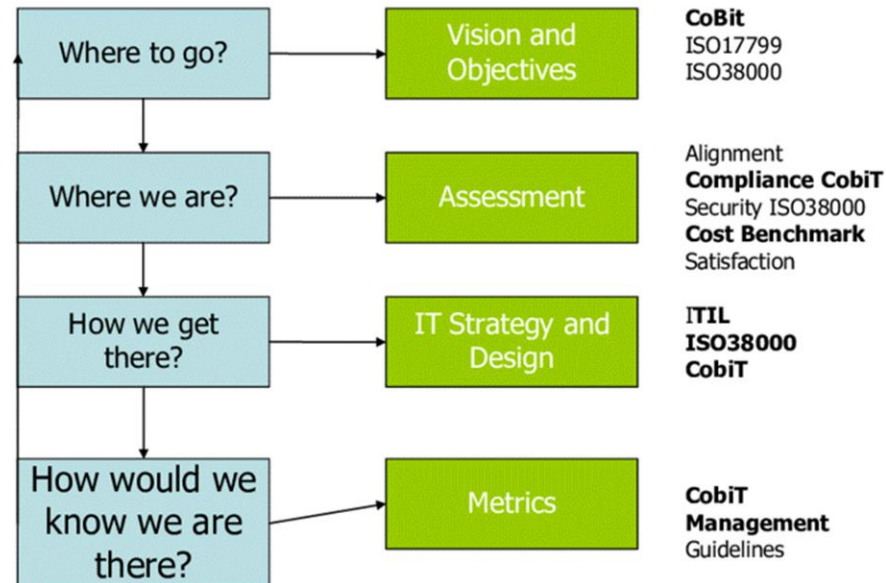
# COMPLIANCE



## Network security risk management

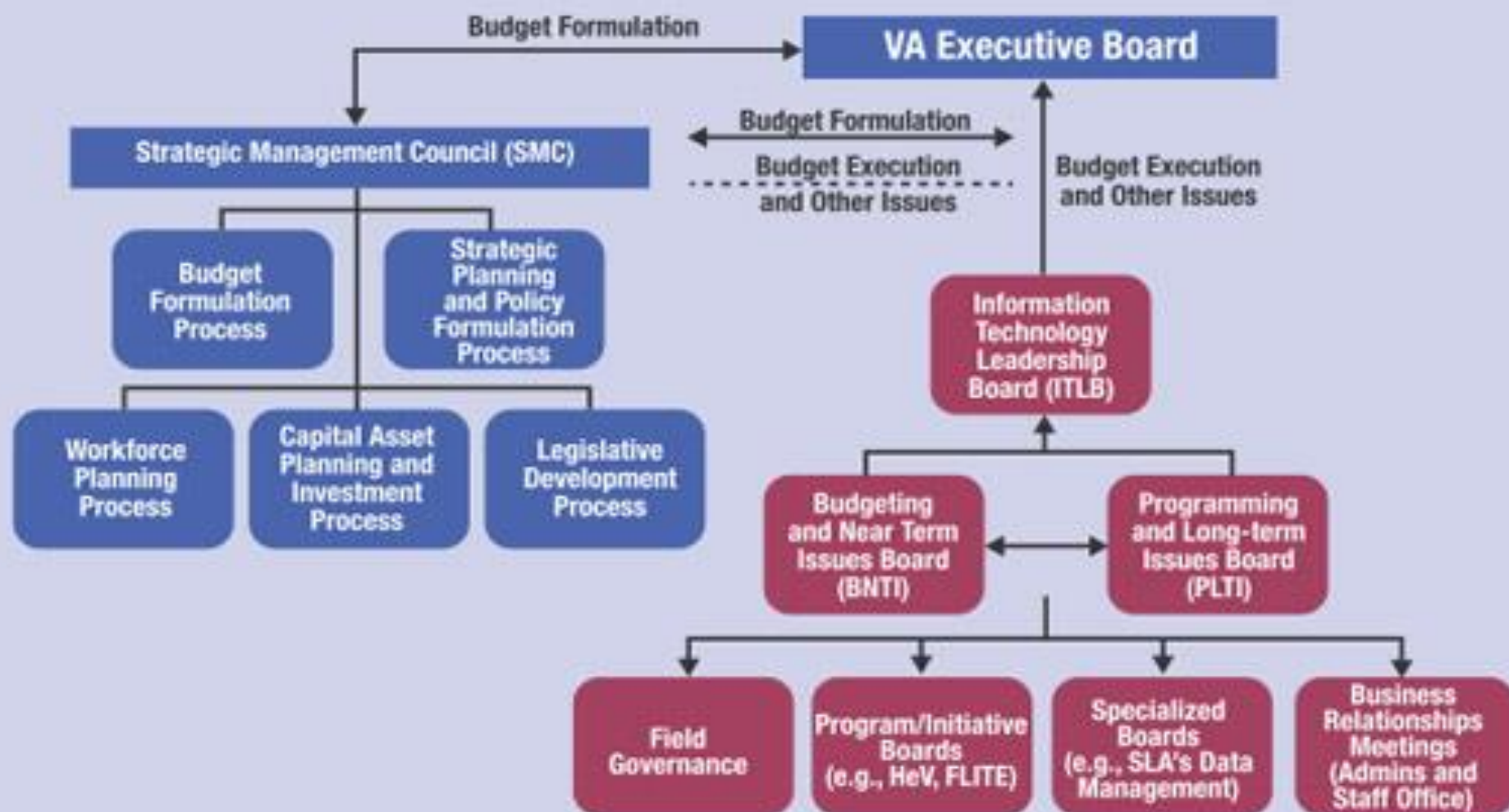


## IT GOVERNANCE FRAMEWORK

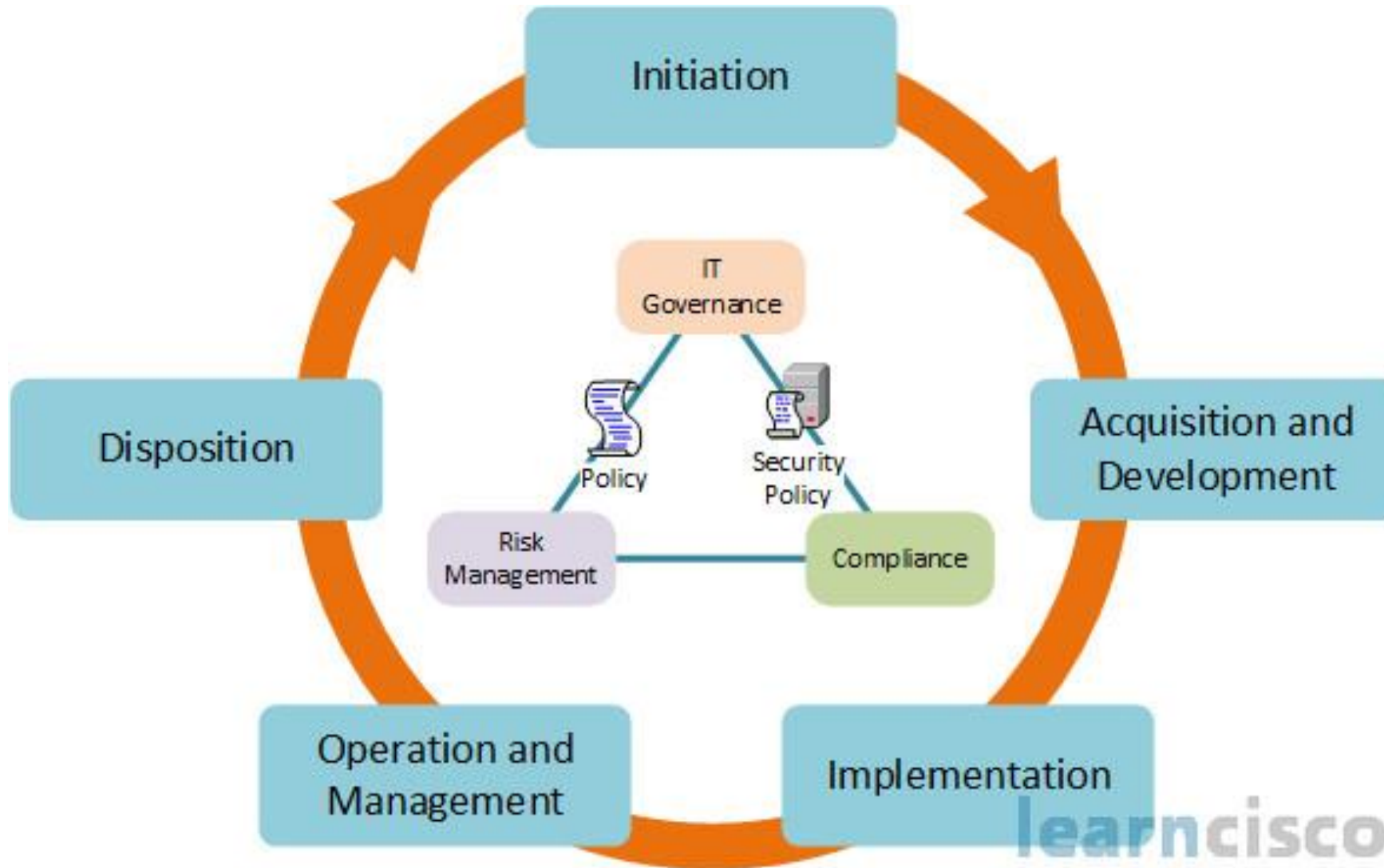


**Figure 4 —VA IT Governance Organizational Structure Example**

**Box 6: IT Governance Structure at VA**



# Secure Network Life-Cycle Management





# Secure Network Life-Cycle Management

- The SNLCM has 5 phases:
  - Firstly the initiation phase
  - Secondly the acquisition and development phase
  - Thirdly the implementation phase.
  - Fourthly is the operations and management phase
  - Fifthly is the disposition phase.

# Initiation Phase

- Categorize security into 3 different levels – low, moderate, or high.
- Project Manager categorizes different areas of the network based on the value of the asset. The value refers to the brand like CISCO and the potential impact on CIA (Confidentiality, Integrity, and Availability).
- In the initiation phase, the preliminary risk assessment is conducted to the initial description of the needs of the system and defining the threat environment where the system operates.

# Acquisition and Development Phase

- In the acquisition and development phase, the risk assessment, risk analysis and security functional requirement analysis are implemented.
  - Component: system security environment
  - what is the existing enterprise security policy, security architecture, functional requirements and assurance requirements (i.e.: legal mandate or under HIPAA or Sarbanes-Oxley or Department of Defense).
  - Cost and budgeting since need to report for all of the stakeholders.
  - Develop supporting documentation, security planning, and you'll develop your security controls – your technical controls, your administrative controls, your physical controls. You'll also develop security testing and evaluation processes, maybe do some penetration testing and auditing. You'll have other planning components as well.

# Implementation Phase

- The implementation phase performs the inspection and acceptance of hardware and software solutions, and system functionality solutions.
- The system integration works well together with all components.
- The deployment and configuration, demand the employee posses a security certification.
- Make sure that staff/employee is certified and accredited.



# Operations and Management Phase

- The operations and management phase performs the configuration management, and configuration control, and continuous monitoring.
- A continual improvement and ongoing operational maintenance is the main task in this phase and it is a day-to-day activities happened.

# Disposition Phase

- In the disposition phase, the project manager needs to determine what information and data are that going to preserve, what systems have to be preserved for how long, based on governance.
- Perform the media filtering – deleting, erasing, and writing over data when necessary on hard drives and removable drives.
- Also, the disposal of hardware and software based on security policy.

# Assessment Phases of the Life-Cycle

- Some most important actions to take to determine the ability to detect, defend, and respond to network attacks.
  - Vulnerability assessment
  - Internal assessment
  - External assessment
  - Access network assessment
  - Operating system and application assessment
  - Security posture assessment and documentation

# Assessment Phases of the Cycle

- In the planning phase – implement an **INTERNAL ASSESSMENT**.
  - In the internal assessment, concentrate on insider threats – either structured or unstructured, malicious or accidental.
  - In the external assessment, focus on packet/events/incidents that come in the perimeter routers in the perimeter firewall systems and come out.
  - Wireless assessment – do you have a wireless network, is your wireless network only a guest VLAN, are you providing wireless solutions for your corporate LAN as well, very important.
  - In security posture assessment
    - analysis and documentation. Documentation in the form of reporting, and metrics, and graphs, technical details using topological maps through things like Microsoft Visio, for example. These are extremely important in assessing your security posture, which knowing where things are, knowing where your critical assets are, and knowing how they are connected.



# Example

## Threats, Vulnerabilities and Mitigations

- **DDoS**
  - Buffer overflow (wrong size packets)
  - SYN requests
  - Block certain IP series
  - Reverse Proxy
  - Transfer all traffic to external company like Akamai
- **Man in the Middle Attack**
  - Especially in WIFI connections
  - Encryption
  - PKI
- **Spoofing**
  - an intruder attempts to gain unauthorized access to a user's system or information by pretending to be the user
  - MFA
  - Clean desk
  - Training

## Threats, Vulnerabilities and Mitigations

- **Alterations**
  - Static Data
  - Applications
  - Traffic
  - Pentesting
  - Source code inspection
  - DB Logging
- **Social Engineering**
  - Shoulder surfing
  - Eavedropping
  - .....
  - Training
- **Ransomware**
- **Virus, worm, malware, Trojan horse, ...**
  - Firewall
  - Active Patch management

# Example

## Data Protection and Mitigations

- **Proxy server**
  - Hide IP outbound addresses
  - Anomous surfing the internet
  - VPN, proxy plus encryption (authentication by logon and password and / or certificate)
- **Reverse Proxy server**
  - Check on inbound IP addresses
- **Certificate Authority**
  - Trustworthiness of parties on the internet
  - Webservers are authenticated (HTTPS)
  - Clients are authenticated (Identity card)
- **Encryption**
  - Symmetric (same encryption key on both sides)
  - Asymmetric (public and private encryption key)
  - Hash algorithm

## Data Protection and Mitigations

- **Intrusion detection and prevention**
  - Checking *afterwards*
  - Tracking what has been affected / which segments were accessed
  - Snort
- **Logging**
  - Tracking and tracing changes / alteration:
  - Data
  - Systems (IT stack)
- **Traffic monitoring**
  - Packet sniffing and protocol analyzer
    - ☑ Snort
    - ☑ Wireshark

# QUALITIES OF PROJECT MANAGER

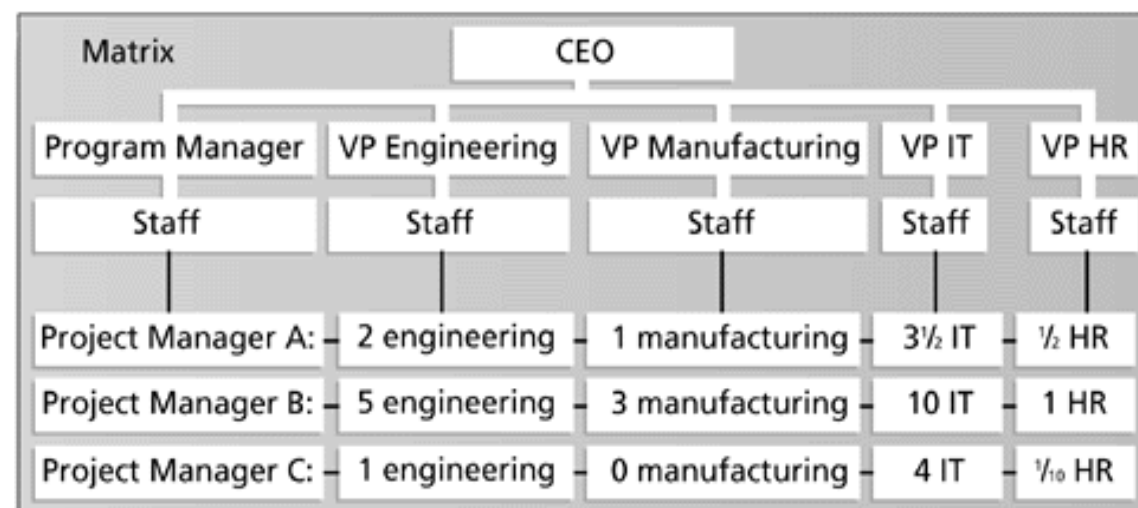
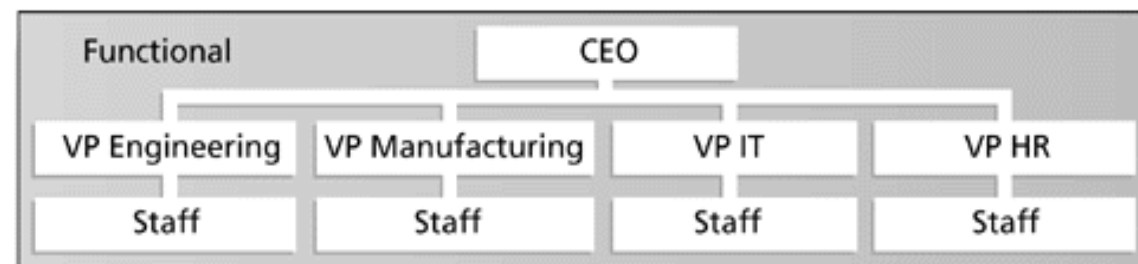
# GOOD QUALITIES OF PROJECT MANAGER

- Communication skills: listening, persuading, helping others
- Organizational skills: planning, goal-setting, analysing
- Team Building skills: empathy, motivation, esprit de corporations
- Leadership skills: sets example, energetic, vision (big picture), delegates, positive
- Coping skills: flexibility, creativity, patience, persistence
- Technological skills: technical experience, project knowledge

# PEOPLE IN THE ORGANIZATION

# Organization Structure

- A project team is a team whose members usually belong to different groups, functions and are assigned to activities for the same project. A team can be divided into sub-teams according to need. Usually project teams are only used for a defined period of time.





**Stakeholder** is a person with an interest or concern in something, especially a business such as investor, president etc.

**Project Leaders** is a person in charge of an information systems project. A project leader uses project management software for keeping track of projects and generally has extensive experience as a programmer, systems analyst or other related informational field. A project leader can sometimes act only as an advisor in the business.

**Team members** are person who responsible for executing tasks and producing deliverables as outlined in the Project Plan and directed by the Project Manager, at whatever level of effort or participation has been defined for them.

# Influence of Organization Structure on Project

<div> <div>Organization Type</div> <div>Project Characteristics</div> </div>	Functional	Matrix			Projectized
		Weak Matrix	Balanced Matrix	Strong Matrix	
Project Manager's Authority	Little or None	Limited	Low to Moderate	Moderate To High	High to Almost Total
Percent of Performing Organization's Personnel Assigned Full-time to Project Work	Virtually None	0-25%	15-60%	50-95%	85-100%
Project Manager's Role	Part-time	Part-time	Full-time	Full-time	Full-time
Common Title for Project Manager's Role	Project Coordinator/ Project Leader	Project Coordinator/ Project Leader	Project Manager/ Project Officer	Project Manager/ Program Manager	Project Manager/ Program Manager
Project Management Administrative Staff	Part-time	Part-time	Part-time	Full-time	Full-time

The organizational structure influences the project manager's authority, but remember to address the human resources, political, and symbolic frames, too.

# FRAMES

# FOUR ORGANIZATION FRAMES

<p><b>Structural frame:</b> Focuses on roles and responsibilities, coordination and control. Organization charts help define this frame.</p>	<p><b>Human resources frame:</b> Focuses on providing harmony between needs of the organization and needs of people.</p>
<p><b>Political frame:</b> Assumes organizations are coalitions composed of varied individuals and interest groups. Conflict and power are key issues.</p>	<p><b>Symbolic frame:</b> Focuses on symbols and meanings related to events. Culture is important.</p>

# THE IMPORTANCE OF PROJECT STAKEHOLDERS

- Recall that project stakeholders are the people involved in or affected by project activities
- Project managers must take time to identify, understand, and manage a good relationships with all project stakeholders
- Using the **FOUR FRAMES** of organizations assist Project Manager to meet stakeholders' needs and expectations
- Senior executives are very important stakeholders

# HIGH COMMITMENT OF TOP MANAGEMENT

- Top management must give a clear picture, clear direction (mission, vision and goals); and assistance to project managers to secure adequate resources, get approval for unique project needs in a timely manner, receive cooperation from people throughout the organization, and learn how to be a better leaders.
- The top management need to be in the same direction and provide facilities for the staff to execute the operation in smooth performance.



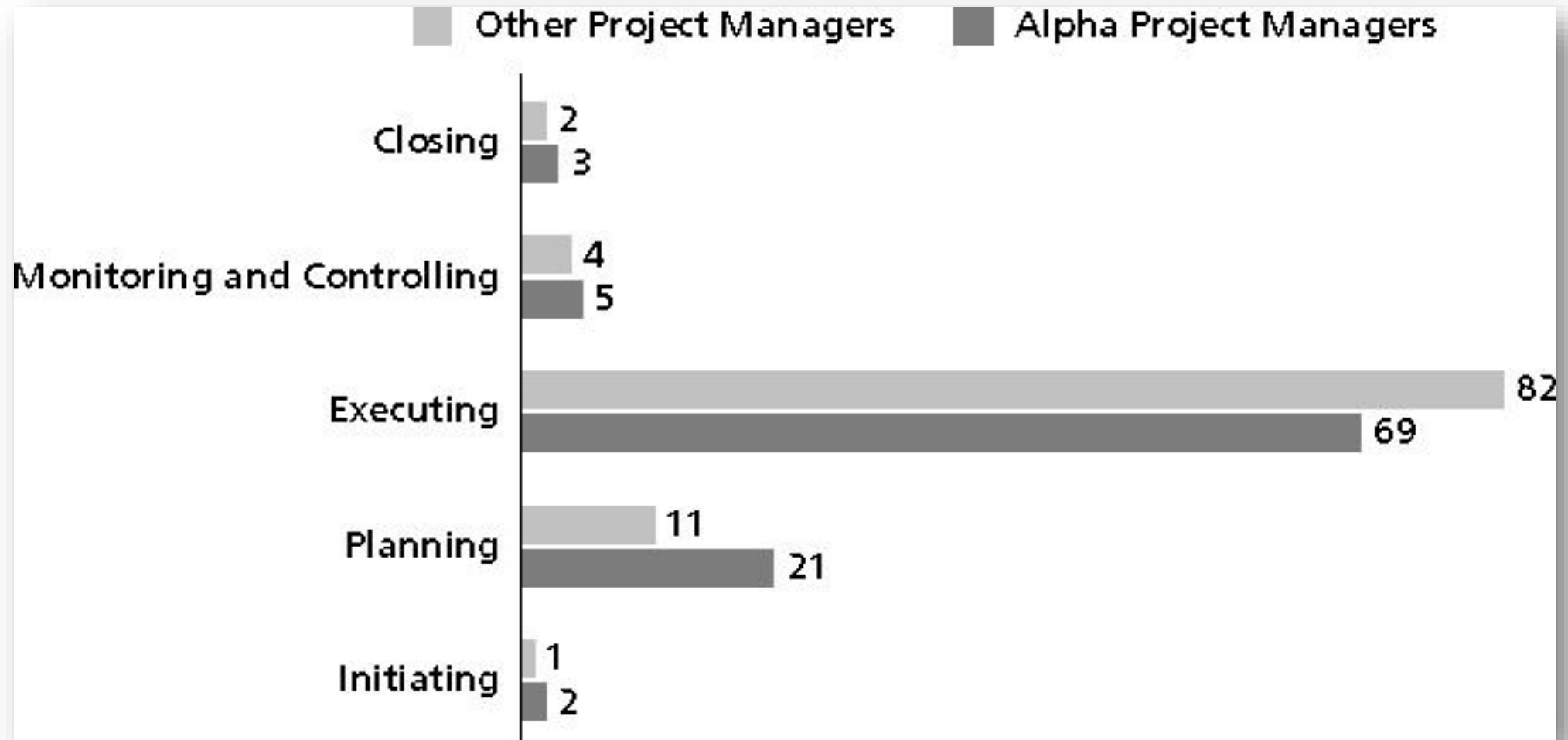
The image features a hand holding a glowing blue network globe, which is composed of interconnected nodes and lines. The background shows server racks with blue and green lights, and a large circular graphic with red dashed lines on the right side. The text "MANAGEMENT OF NETWORK SECURITY PROJECTS PROCESS" is overlaid on the image in a bold, sans-serif font. The words "MANAGEMENT OF" and "PROJECTS" are in yellow, while "NETWORK SECURITY" and "PROCESS" are in white.

# MANAGEMENT OF NETWORK SECURITY PROJECTS PROCESS

# PROCESS GROUP

- A process is a series of actions directed toward a particular result
- Project management can be viewed as a number of interlinked processes
- The project management process groups include
  - initiating processes
  - planning processes
  - executing processes
  - controlling processes
  - closing processes

# PERCENTAGE OF TIME SPENT ON EACH PROCESS GROUP



# MAPPING THE PROCESS GROUPS TO THE KNOWLEDGE AREAS-1

Knowledge Area	Project Management Process Groups				
	Initiating	Planning	Executing	Monitoring and Controlling	Closing
<i>Project Integration Management</i>	Develop project charter	Develop project management plan	Direct and manage project execution	Monitor and control project work, Perform integrated change control	Close project or phase
<i>Project Scope Management</i>		Collect requirements, Define scope, Create WBS		Verify scope, Control scope	
<i>Project Time Management</i>		Define activities, Sequence activities,		Control schedule	

\*Source: PMBOK® Guide, Fourth Edition, 2008.

# MAPPING THE PROCESS GROUPS TO THE KNOWLEDGE AREAS-2

Knowledge Area	Project Management Process Groups				
	Initiating	Planning	Executing	Monitoring and Controlling	Closing
<i>Project Time Management (continued)</i>		Estimate activity resources, Estimate activity durations, Develop schedule			
<i>Project Cost Management</i>		Estimate costs, Determine budget		Control costs	
<i>Project Quality Management</i>		Plan quality	Perform quality assurance	Perform quality control	
<i>Project Human Resource Management</i>		Develop human resource plan	Acquire project team, Develop project team, Manage project team		

# MAPPING THE PROCESS GROUPS TO THE KNOWLEDGE AREAS-3

<i>Project Communications Management</i>	Identify stakeholders	Plan communications	Distribute information, Manage stakeholders expectations	Report performance
<i>Project Risk Management</i>	Plan risk management, Identify risks, Perform qualitative risk analysis, Perform quantitative risk analysis, Plan risk responses			Monitor and control risks
<i>Project Procurement Management</i>	Plan procurements	Conduct procurements	Administer procurements	Close procurements



# THE END

Thank you