

ICT Governance and Performance Management

CSU 08211

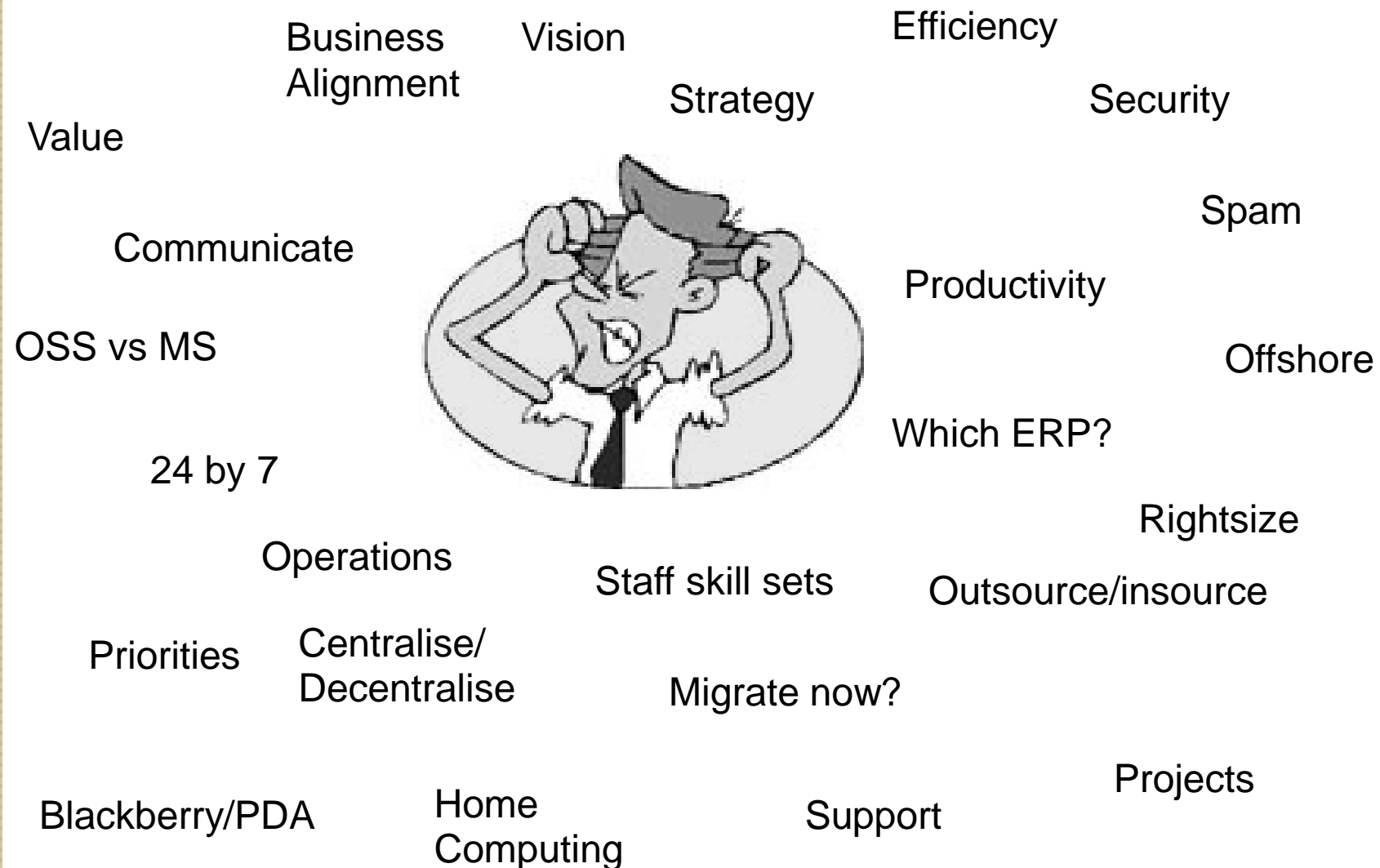
COMPUTER SYSTEMS MANAGEMENT
II

Governance - Definition

WordNet Dictionary

Definition: the act of governing exercising authority; the persons (or committees or departments, etc.) who make up a body for the purpose of administering something;

The Beleaguered CIO!



The IT Governance team!

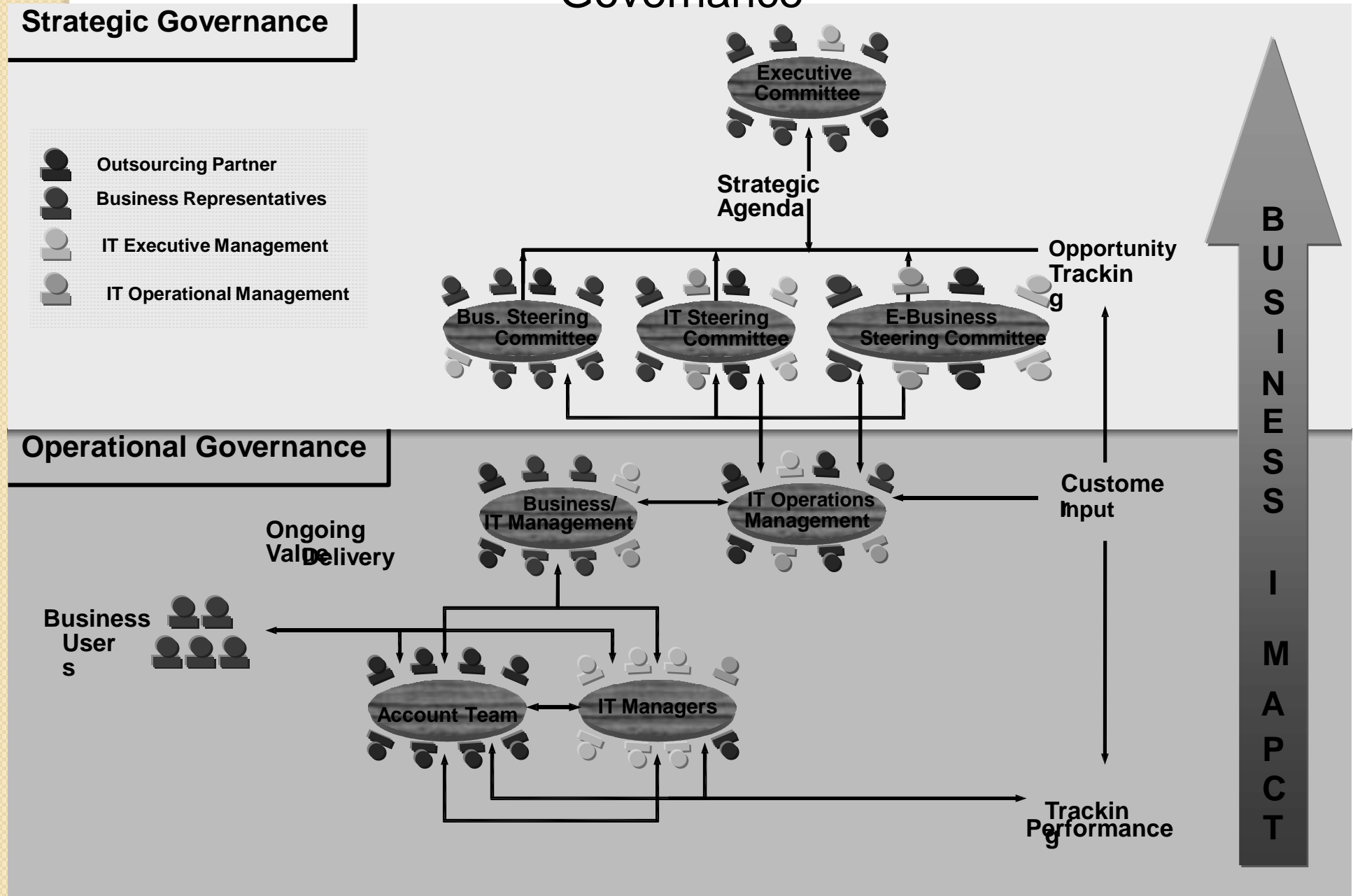


"OK, all those in favour of delegating decision-making, shrug your shoulders"

Who is responsible for IT Governance?

“IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategies and objectives.”

Give Soft Relationships A Harder Structure Through Joint Governance

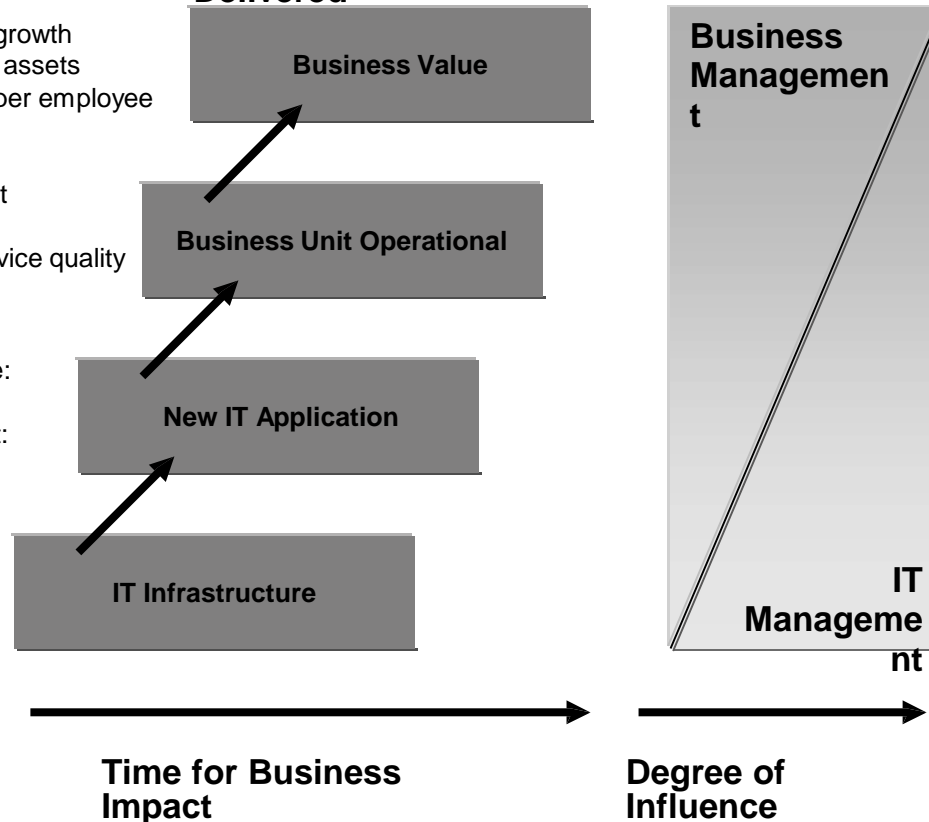


Good Governance Is A Foundation For Good Management – Not A Substitute For It

Sample Measures

- Revenue growth
- Return on assets
- Revenue per employee
- Time to market
- Sales
- Product or service quality
- Implementation time: new application
- Implementation cost: new application
- Infrastructure availability
- Cost per transaction
- Cost per workstation

Business Value Delivered

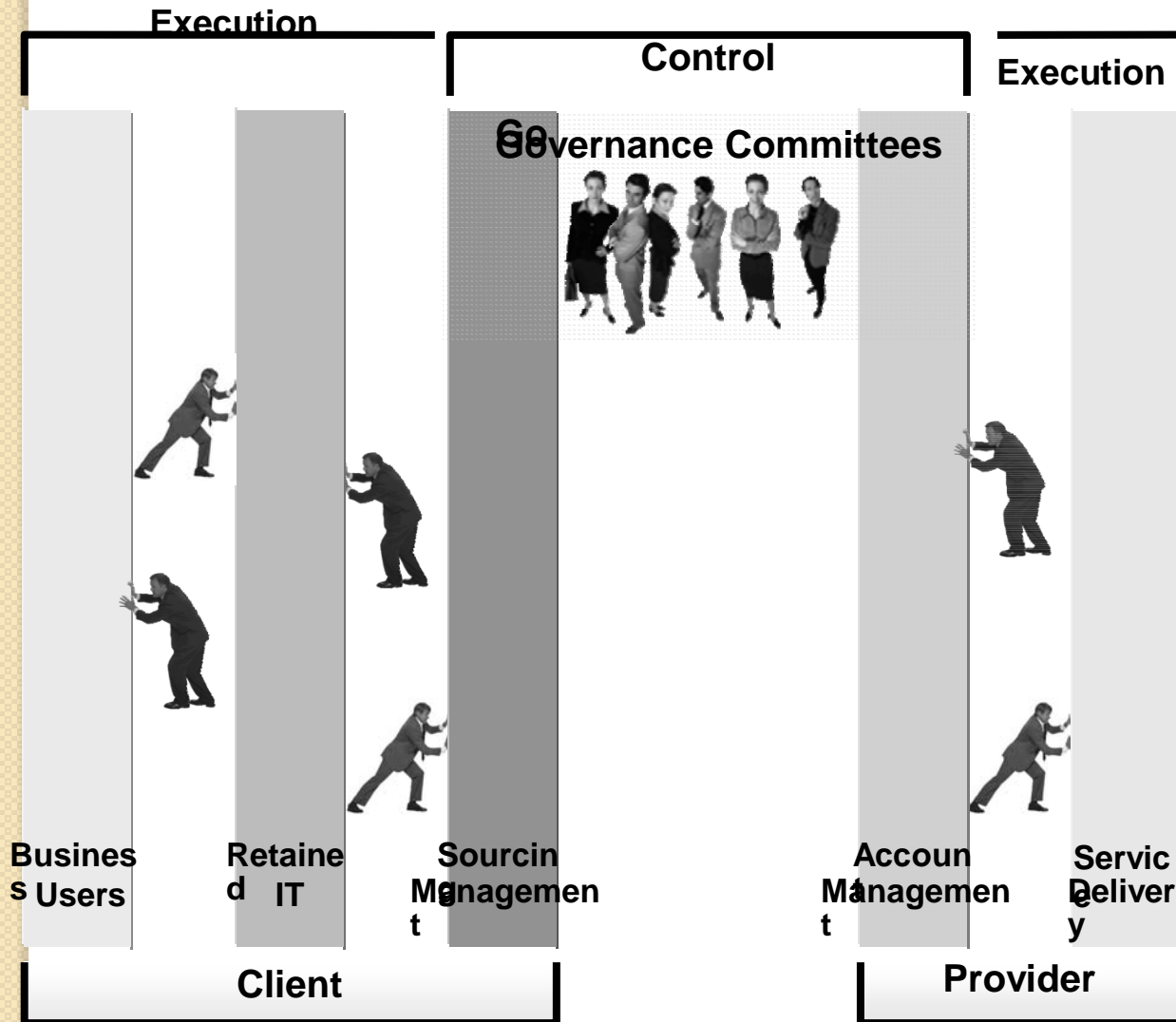


Good governance:

- Is not just a structure for making decisions; it is an active process for creating alignment
- Is not all formal enforcement; it is mainly informal and enabling

Poor Governance Leads To Poor Performance – Outsourcing Makes It Worse

Standard Outsourcing Governance



- IT and business isolated from each other
- Outsourcing provider kept on the outside
- Accountability not clear
- Poor communications
- No mechanisms for collaboration and innovation
- Lack of leadership and stakeholder buy-in

“The politics are hell!” – Chemicals Group CIO

At worst ...

- The business ignores the dilemmas and IT is torn between conflicting requirements

Commonly...

- IT is used as a ‘Trojan horse’ for the standardization of business practices

At best ...

- IT is asked to resolve conflicts that the business is unable to sort out for itself

And by the way...

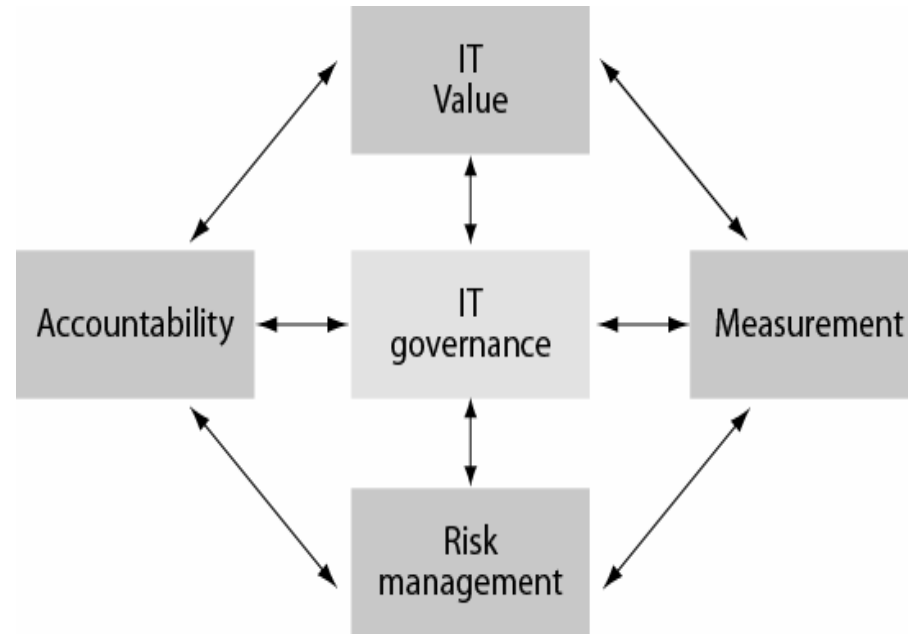
- IT probably has its own version of the global/local dilemma inside its organization



Welcome to the Governance team!



The Four Dimensions Of IT Governance



How does Governance ensure that IT delivers business value? How do you align with business strategy?

- If Orgs value proposition is built on IT, are the risks associated with IT the same as risks to the business? – security, privacy, identity theft...
- Does IT governance hold IT management accountable for the return on investment in IT?
- Do IT value metrics help enforce IT alignment with business? Do operational excellence metrics help manage risks?

More Discussion Points

- What Governance Structure do you have in your Organisation?
Does it make a difference?
- We appear to do a good job at operational governance but what about at the business strategic level?
- Should the CIO be sitting at the table with senior managers?
- Given the many challenges facing the CIO, is anarchy a choice?
- How do you measure the value of IT? Do IT metrics have the credibility?
- Are ICT managers really in control of their organisation or does the industry

- 
- IT PERFORMANCE MANAGEMENT
 - THE CONCEPT AND PROCEDURES



what best practices lead to efficient and effective management of computer systems?

- The best practices help define what is needed for effectively managing computer systems in ways that optimize the systems' use and control their risks.
- Best practices for managing computer systems address policy, staffing, and security issues.



Best Practices for Managing Computer Systems

1. A Framework Should Be in Place to Guide the Management of a Computer System
2. Knowledgeable Staff Should Maintain and Use the Computer System
3. Computer Systems Should be Secure



I. A Framework Should Be in Place to Guide the Management of a Computer System

- Inventories should clearly identify computer equipment and software, and standards should be set
- Key policies, procedures, and the current operating environment should be documented
- Policies and procedures should be communicated to staff
- Adherence to computer system policies and procedures should be monitored
- Policies and procedures should be regularly reviewed and updated

Sample hardware inventory

A database of hardware inventory might include the following elements:

- Information on the manufacturer, model, and serial number (or some other unique identification number)
- Equipment description (possibly with a menu of predefined choices to preserve consistency) by category, such as desktop computer, laptop computer, or printer
- Comment field (may include a history of who has had the equipment or, in the case of lost or stolen equipment, details of what occurred and pointers for police reports)
- Information on the purchase date and purchase order number to establish time period for the warranty
- Configuration information, including disk size and amount of memory, based on the device machine name, if any
- Internet protocol (IP) name and IP address
- Location code and physical location, such as room number
- User name and ID (does not apply for network and multi-user components)
- Organizational affiliation, such as the department or unit
- Owner history, if applicable
- Usability code or condition (e.g., in current use, ready to reassign, ready to dispose of, scrapped for parts, retired, lost, stolen)

Key Management Program Components

Component	Description
Asset Management	Track hardware and software owned and whether they are in use
Technology Standards Management	Set product standards that ensure system reliability and compatibility
Software Licensing Control	Ensure compliance with licensing laws
Systems Management	Ensure that hardware and software configurations are current, documented, and performing as expected
Systems Administration	Ensure that user IDs are current, access is appropriate, and that storage capacity is kept at required levels
Change Management	Ensure that system changes do not interfere with reliable operation and availability
Security Management and Virus Protection	Protect the jurisdiction from data loss and systems damage due to hacking, theft, or virus attacks
Disaster Recovery and Contingency Planning	Protect the jurisdiction in the event of a systems outage or loss of critical data
End-User Support	Resolve technical problems and assist in the use of technology



2. Knowledgeable Staff Should Maintain and Use the Computer System

- The expertise of technology staff should be assessed
- A recruitment and retention process should be in place for technology staff
- Training for technology staff should be ongoing
- User training should be available
- User support should be provided

User Support Strategies

- Awareness meetings to introduce computer system goals and features
- Easy to follow, one-page “cheat sheets” for common activities
- Small group training, review, and support sessions
- Frequently-asked question and answer brochures
- On-line help features including discussion groups, e-mail, video, and intranets
- Designated learning time for new employees
- Individual tutoring or peer tutoring
- A help newsletter
- Full-scale documentation manuals
- Videotaped step-by-step instruction
- Computer system maps presented graphically and in color
- A staffed help desk



3. Computer Systems Should be Secure

- A risk assessment should be conducted and security policies should be based on it
- User accounts should be managed and procedures should identify who may modify equipment or system data
- Firewalls and antivirus software should be employed and monitored
- A disaster recovery plan should be developed and back-up procedures should be conducted
- The security plan should be tested
- Trained professionals should plan, monitor, and enforce security

Elements of a Computer Use Policy

A computer use policy should define the extent to which users may:

- Make hardware changes
- Install or remove software
- Perform work outside the ordinary scope of business or their job description
- Use specific network services, such as e-mail and Internet access
- Transmit information across the network, including e-mail, attachments, and downloaded files
- Make configuration changes if employees are given higher levels of access

Plus, the policy should describe how users are to operate the computer in line with specific security requirements, such as using a password-protected screen saver or turning the computer off at the end of the work day.



Elements in a Password Policy

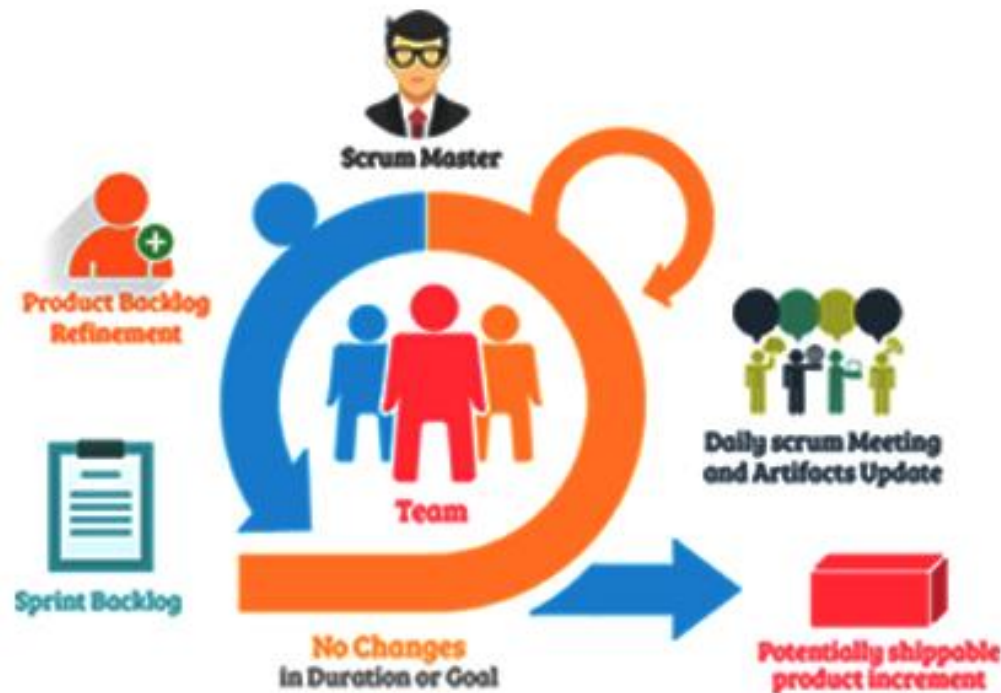
- **Length:** Set a minimum length for passwords, such as eight characters.
- **Complexity:** Require a mix of characters, such as requirements to contain both uppercase and lowercase letters and at least one nonalphabetic character.
- **Aging:** Determine how long a password may remain unchanged. For instance, require users to change their passwords every 30 to 45 days.
- **Reuse:** Decide whether a password may be reused to prevent employees from repeatedly using the same passwords. Limit the number of times a person may reenter passwords to prevent unauthorized users from gaining access to the system.
- **Authority:** Determine who is allowed to change passwords and delete user accounts when users leave an agency.

System performance

- When considering system performance, several issues have to be monitored, including
 - Network
 - Workstations
 - Servers
 - Applications
 - Server version software
 - Database
 - Information systems
- All of these require governance and monitoring tools which includes **POLICIES** and **PROCEDURES**

How to achieve top

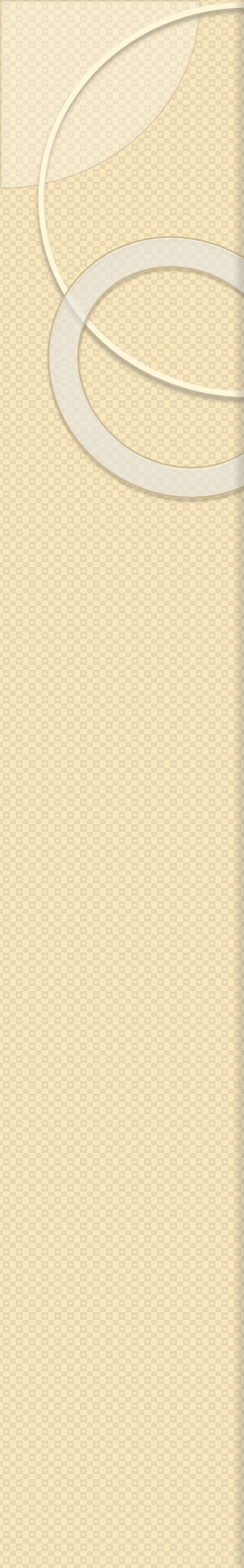
BE AGILE!



- Across the globe, there is a lot of **hype around different methodologies of performance management** – from traditional methods of project management, to the now globally accepted **AGILE APPROACH**.

What is the difference between traditional and Agile methodology?

- **Traditional methodologies** are carried out in stages, where one stage follows the previous one and there are no iterations. Many people criticize this methodology, especially when it comes to software development, because it makes it necessary to precisely plan out every detail and feature before going into development, and making changes later in the process is either impossible or very expensive.
- **Agile methodology** argues that it is good to make changes during the development process and that changes should be made constantly because they bring improvement. Also, iterative development reduces the cost of these changes, because a change in a small segment of the project costs a lot less than a change on a finished project. It's because of these characteristics that this is called Agile methodology.

- 
- The whole issue of performance management is to make sure that
 - IT systems are scalable
 - Tunes, Tested and Monitored.
 - In order to identify system
 - Performance (speed)
 - Scalability (increased output)
 - Capacity (maximum level of output)
 - Bottleneck (resources limiting the performance)

Required skill set

- Tuning
- Testing
- Configuration