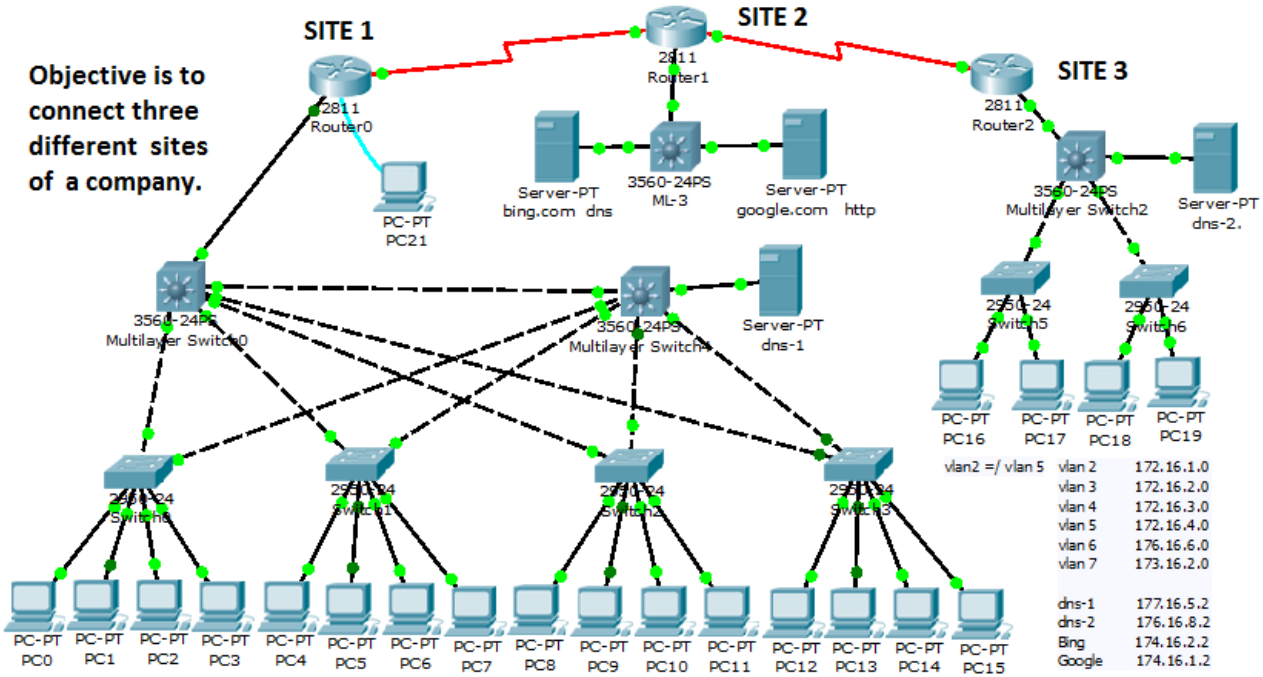
IT2775 Operations Security

Configuration and Change Management

NANYANG POLYTECHNIC

Objectives

- Purpose & Goal of Configuration Management
- Essential Elements of Configuration Management
- Change Management Process



Configuration Management (CM)

- Purpose:
  1) To maintain data and report status of identified configuration units (CU).
  2) To analyze and control changes to the system and its configuration units.

- Goal:
  1) To maintain control over operations.
  2) To maintain the security level of IT operations.

Essential Elements of CM

1. Establish Config Mgmt methodology
2. Identify Configuration Units (CU)
3. Maintain work product **baselines**
4. Control changes to established CU
5. Communicate configuration status

baseline

['beɪslʌɪn]

NOUN

1. a minimum or starting point used for comparisons.

1. Establish Config Mgmt Methodology

- How should the organisation do CM?
  - Level of detail (CU: physical server or MSSQL)
  - When to add to CM? (upon purchase or deployment)
  - Level of formalization (structured vs. cost/time)
- Identify automated tools to assist in process.
  - Extract relevant information from the CU directly.
  - Manage CM information e.g. database.
  - Audit CU for compliance.

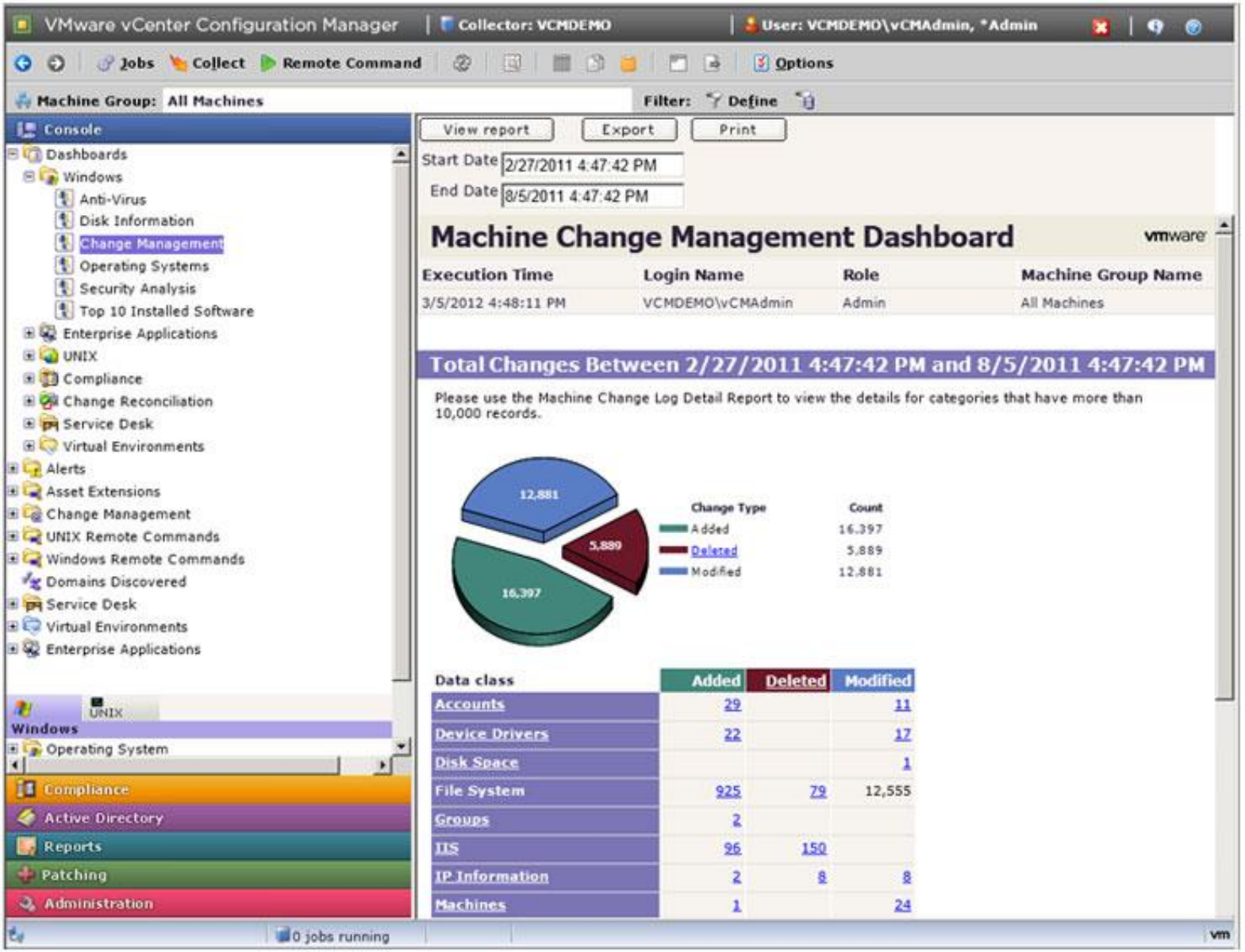
2. Identify Configuration Units

- CU: Objects that are tracked for CM.
  - Significant assets of the organisation.
  - PC, network/security devices, core business s/w.
- Information captured
  - Hardware
    - Make & Model
    - MAC address
    - Serial no
    - OS & firmware version
    - Physical location
    - BIOS and related passwords
    - Assigned IP address
  - Software
    - Name and Publisher
    - Date purchased/deployed
    - Machines installed
    - Version and service pack
    - Licensing details
    - Configuration settings
    - S/w Dependences

3. Maintain CU Baselines

- Baseline – collection of standard-configurations of production CUs.  Video on Baselines
- Establish procedures to
  - add, delete and update to the baseline
  - monitor and audit configuration data
  - document and trace rationale of change
- Outcomes:
  - baselined CUs.
  - triggers to update CUs, rectify improper procedures.
  - documented CU updates and decisions.

AUTOMATE !!!


VMware vCenter Configuration Manager
Collector: VCMDEMO
User: VCMDEMO\vCMAdmin, *Admin
Jobs
Collect
Remote Command
Options
Machine Group: All Machines
Filter: Define
Console
Dashboards
Windows
Anti-Virus
Disk Information
Change Management
Operating Systems
Security Analysis
Top 10 Installed Software
Enterprise Applications
UNIX
Compliance
Change Reconciliation
Service Desk
Virtual Environments
Alerts
Asset Extensions
Change Management
UNIX Remote Commands
Windows Remote Commands
Domains Discovered
Service Desk
Virtual Environments
Enterprise Applications
Windows
Operating System
Compliance
Active Directory
Reports
Patching
Administration
View report
Export
Print
Start Date 2/27/2011 4:47:42 PM
End Date 8/5/2011 4:47:42 PM
Machine Change Management Dashboard
vmware
Execution Time
Login Name
Role
Machine Group Name
3/5/2012 4:48:11 PM
VCMDEMO\vCMAdmin
Admin
All Machines
Total Changes Between 2/27/2011 4:47:42 PM and 8/5/2011 4:47:42 PM
Please use the Machine Change Log Detail Report to view the details for categories that have more than 10,000 records.
12,881
5,889
16,397
Change Type
Count
Added
16,397
Deleted
5,889
Modified
12,881
Data class
Added
Deleted
Modified
Accounts
29
11
Device Drivers
22
17
Disk Space
1
File System
925
79
12,555
Groups
2
IIS
96
150
IP Information
2
8
8
Machines
1
24
0 jobs running

4. Control Changes to Established CU

- Maintain control over CU changes.
  - Change requests are analysed to determine the impact (with other CUs), with costs and schedule.
    - Approval process can be shorter for changes that do not affect other CUs.
  - After formal approval, schedule and implement the change.
- Outcomes:
  - Revised product baselines ie. updates!

5. Communicate Configuration Status

- Inform all affected by changes to the CU.
  - Organisation's operations depends on accurate information.
  - When the changes will be processed?
  - What associated CUs will be affected?
  - Developers, customers and all who need to know.
- Outcomes:
  - Status reports showing the changes made
  - Evidence of communicating reports to relevant parties.

Essential Elements of Config Mgmt (CM)

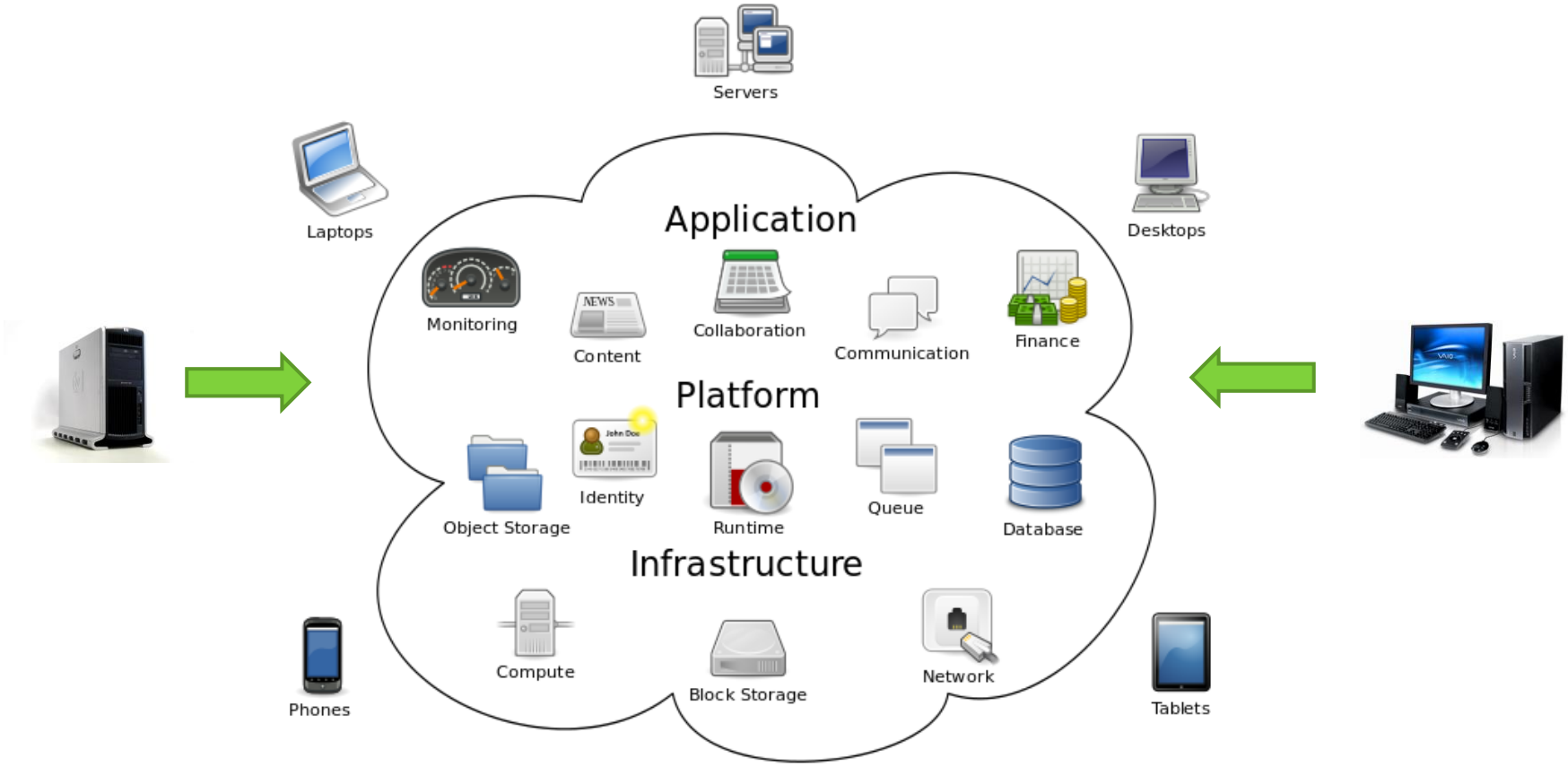
1. Establish CM methodology
2. Identify Configuration Units (CU)
3. Maintain CU baselines*
4. Control changes to established CU*
5. Communicate configuration status*

* Change management happens here

Video on Change Mgmt

Change Management

- Changes can introduce vulnerabilities in a secured operating environment.



Change Management

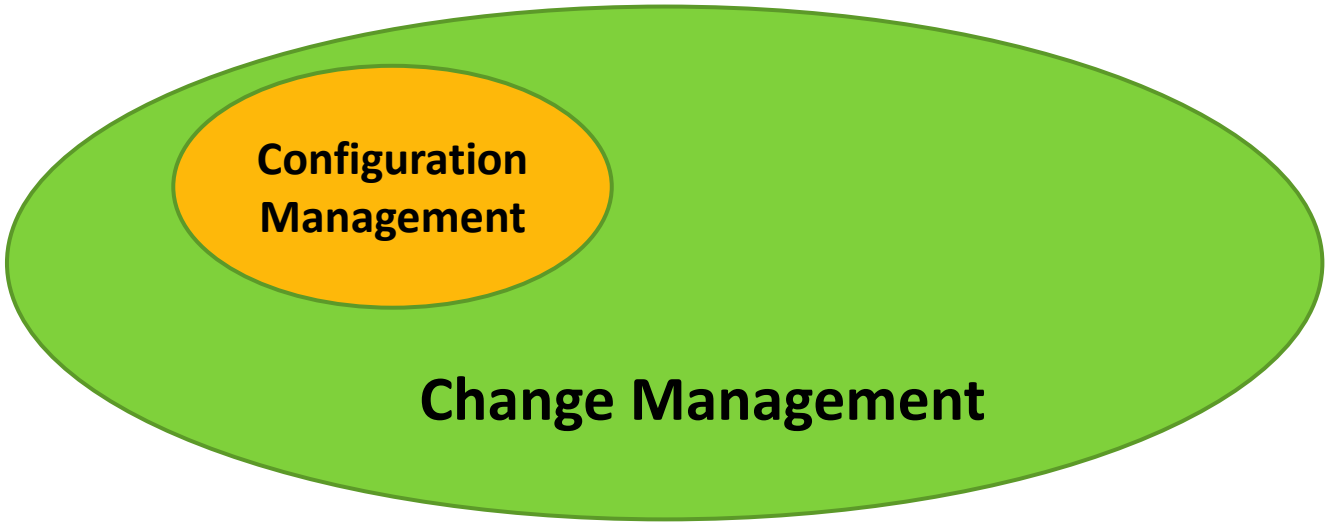
- Changes can introduce vulnerabilities in a secured operating environment.
  - **systematically manage change to maintain security.**
    1) monitored, orderly and controlled manner.
    2) effects of changes are systematically analysed.
    3) negative impact of changes is minimized.
    4) formalized testing to verify against expected results.
    5) changes are reversible.
    6) users are informed prior to changes.
  - **involves planning, testing, auditing and monitoring**.

Change Management

- Develop and implement in the organisation
  - procedures for specific aspects of changes, e.g. business core, projects, patch mgmt or CM.
  - processes to chain up the procedures into workflows.
  - policies to ensure processes are followed.
- Change management should be codified as an organizational policy.
  - championed by senior management eg. CIO / CTO

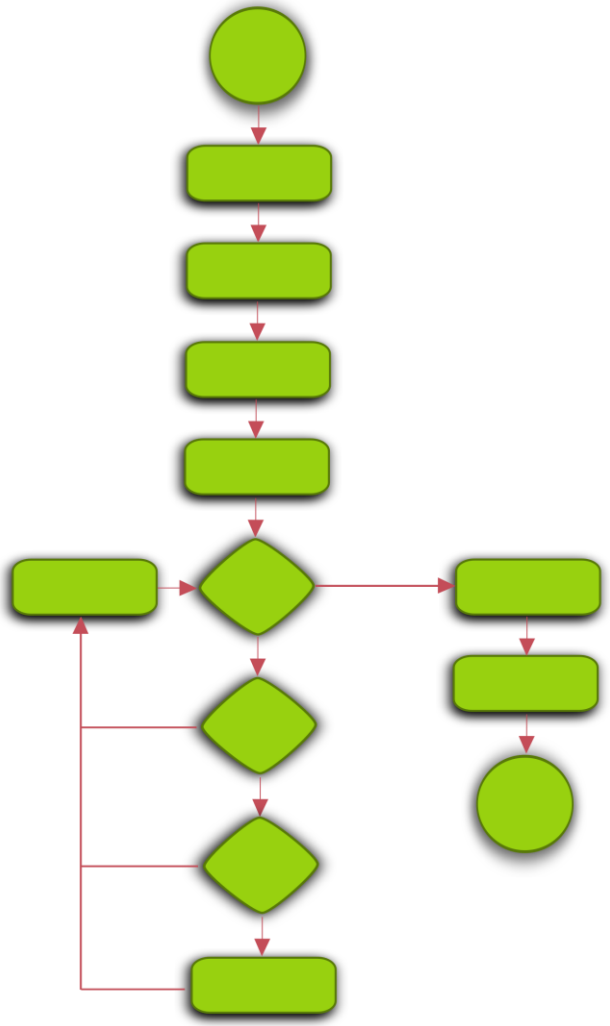
CM vs. Change Management

- CM: focus on managing changes to hardware and software configurations (specific instance)
- Change Mgmt: focus on managing changes in general (bigger picture)
- Configuration Management is a specific instance of Change Management



Change Management Process

1. Change Request
2. Assess Impact
3. Approval
4. Build and Test
5. Notification
6. Implementation
7. Validation
8. Documentation



Change Management Process

1. Change Request
   - formally requested in writing or electronically.
   - change details, business and technical justifications, benefits and projected costs.
2. Assess Impact
   - Approving committee analyses impact of proposed change (time, costs, indirect issues) on operations.
     - Reassess the threats and vulnerabilities if change is implemented.
     - If vulnerabilities are identified, assess risks and potential mitigations.

Change Management Process

3. Approval
   - To be officially approved or rejected.
   - May be postponed if further investigations needed.
   - Impact analysis and decision documented for subsequent similar change requests or audits.
4. Build and Test
   - Prior to implementation, changes are tested in non-production environment and results documented.
   - Perform security review of the changes to ensure no vulnerabilities are introduced.
   - Similarly for requests to remove software or systems.

Change Management Process

5. Notification
   - Inform affected users of proposed change and the schedule of deployment.
   - Notification recorded as proof of action.
6. Implementation
   - Need to be done incrementally, step-by-step. This eases troubleshooting if things go wrong.
   - Implementation should take into account usage patterns of the affected system and be scheduled during lull periods.

Change Management Process

7. Validation
   - Operations staff validates that intended machines received the deployment package of changes.
   - May be manual or automated.
   - Perform security review of affected machines to validate that the security level is as expected.
   - Monitor issue tracking system until no new issues.
8. Documentation
   - Record change details, outcome and lessons learnt.
   - Can be integrated with configuration management.

Examples of Change Requests

- Buy new workstation for staff
- Add additional storage for server
- Shift data centre to another location
- Acquire new payment terminals eg. POS
- Acquire new software
- Replace old terminals
- Upgrade application systems
- Upgrade Windows 7 to Windows 10

Summary

- Purpose & Goal of Configuration Management
- Essential Elements of CM
  1. Establish CM methodology
  2. Identify CU
  3. Maintain CU baselines
  4. Control changes to established CU
  5. Communicate configuration status
- Change Management Process
  1. Request
  2. Assess Impact
  3. Approval
  4. Build and Test
  5. Notification
  6. Implementation
  7. Validation
  8. Documentation