1. **OverView & Best Practices**
   1. Task Sequence is a set of steps ran from top to bottom in order to complete a task such as installing an Operating System.
   2. The order of the steps matters!!
   3. It is best to group like steps together under 1 folder.
2. **Using Logic in a Task Sequence**
   1. Using Logic can allow you to create steps that will only work in certain situations (Mfr.,model,boot,etc.)
   2. Two Main Types of Logic Used in Task Sequences
      1. WMI (Windows Management Instrumentation) Query
      2. Task Sequence Variable – Can be standard or created manually
3. **WMI Queries**
   1. Manufacturer: Select \* from Win32\_ComputerSystem WHERE Manufacturer Like "%Dell%"
   2. Model: Select \* from Win32\_ComputerSystem WHERE Model Like "%Optiplex%"
   3. Partition: SELECT \* FROM Win32\_LogicalDisk WHERE Name = "C:" AND DriveType = 3
   4. Negative Query: SELECT \* From Win32\_ComputerSystem WHERE NOT Model Like "%Optiplex 980%"
4. **Task Sequence Variables**
   1. **Useful Built-in Task Sequence Variables**
      1. \_SMSTSLaunchMode: Checks how task sequence was launched. SMS=Device Collection UFD=USB
      2. \_SMSTSBootUEFI: Returns true if computer BIOS is in UEFI Mode
   2. **Creating Custom Built-in Variables**
      1. Create TS Variable using Powershell: $tsenv.Value("VariableName")="Value"
      2. Use TS Variable in a command, put %% around variable name Example: x:\CCTK\cctk.exe --asset=%VariableName%
5. **Setting BIOS Settings**
   1. **Dell**
      1. Use Dell Command Configure to set BIOS settings for all Optiplex, Latitude, and XPS models
      2. Use Dell Command Configure GUI to set BIOS settings and save them to an ini file.
      3. Task Sequence step can be run in Windows PE environment
      4. Set BIOS setting through ini file command: cctk.exe –i name.ini –valsetuppwd=Password
   2. **HP**
      1. Use the HP BIOS Configuration Utility which works across all HP Business Models
      2. You do not set BIOS settings with the utility, but instead setup a computer with the settings you want and then export the settings to a file. The BIOS Utility can import the file through a TS.
      3. Task Sequence step can be run in Windows PE environment
      4. Example TS Step: x:\HP\BiosConfigUtility64.exe /set:"x:\HP\hpuefi.txt" /cspwdfile:"x:\HP\password.bin"
   3. **Lenovo**
      1. Lenovo has separate BIOS Utilities per model type.
      2. You do not set BIOS settings with the utility, but instead setup a computer with the settings you want and then export the settings to a file. The BIOS Utility can import the file through a TS.
      3. TS Step CANNOT be run in Windows PE and has to be run after the OS is installed
      4. Example TS Step: cmd /c cd c:\lenovo\M900\_BIOS & cmd /c srwin.exe /r m900.dat /ign /nor
6. **UEFI**
   1. A computer CANNOT be switched from Legacy Mode to UEFI Mode in the middle of a Task Sequence
   2. Best way to automate conversion to UEFI is to create separate Task Sequence to switch computer to UEFI before main Task Sequence starts
7. **Windows 10**
   1. List of Windows 10 Customizations: <http://garytown.com/windows-10-customizations-during-osd>
   2. Files for all COB Windows 10 Customizations:

<https://oat.sharepoint.illinoisstate.edu/sccm/SitePages/Home.aspx> -> Shared Departmental Documentation-> COB -> Task Sequences-> COB Windows 10 Task Sequence Settings

1. **BitLocker**
   1. Allows you to do hard drive encryption and export the key to Active Directory
   2. In order to enable BitLocker, you need to add 7 steps to your account.
      1. Run PowerShell script setTasksequenceVariables which can be downloaded at: <https://oat.sharepoint.illinoisstate.edu/sccm/SitePages/Home.aspx> -> Shared Departmental Documentation-> COB ->BitLocker Setup->BitLocker PowerShell Scripts
      2. Disable BitLocker Step: Will disable BitLocker if BitLocker is enabled, needs to be run in Windows
      3. Create 2nd Hard Drive Partition: BitLocker needs at least a 300 MB non OS partition to use correctly
      4. Set a BIOS Password: BitLocker needs a BIOS password to order enable TPM chip
      5. Enable & Activate TPM Chip: BitLocker needs a TPM Chip enabled and activated in BIOS in order to encrypt drive. This can be done on Dell’s with Command Configure Utility.
      6. Pre-provision BitLocker: Will pre-provision the 2nd partition for BitLocker before OS is installed; allows for faster encryption during Enable BitLocker step
      7. Enable BitLocker: Will finish encrypting the drive and export the key to Active Directory.
2. **Additional Documentation**
   1. Windows 10 Task Sequence Steps:

<https://oat.sharepoint.illinoisstate.edu/sccm/SitePages/Home.aspx> -> Shared Departmental Documentation-> COB ->Task Sequences-> COB Windows 10 Task Sequence Steps

* 1. Windows 10 BitLocker Task Sequence Steps: <https://oat.sharepoint.illinoisstate.edu/sccm/SitePages/Home.aspx> -> Shared Departmental Documentation-> COB -> Task Sequences-> COB Windows 10 BitLocker Task Sequence Steps
  2. UEFI Conversion Task Sequence Steps:

<https://oat.sharepoint.illinoisstate.edu/sccm/SitePages/Home.aspx> -> Shared Departmental Documentation-> COB -> Task Sequences-> COB UEFI Pre-Build Task Sequence Steps

* 1. Setting BIOS Settings on Dell, Lenovo and HP’s:

<https://oat.sharepoint.illinoisstate.edu/sccm/SitePages/Home.aspx> -> Shared Departmental Documentation-> COB -> Task Sequences-> Set BIOS settings for Dell, Lenovo, HP in Task Sequence

* 1. Setup BitLocker with SCCM:

<https://oat.sharepoint.illinoisstate.edu/sccm/SitePages/Home.aspx> -> Shared Departmental Documentation-> COB->BitLocker Setup-> Setup BitLocker with SCCM