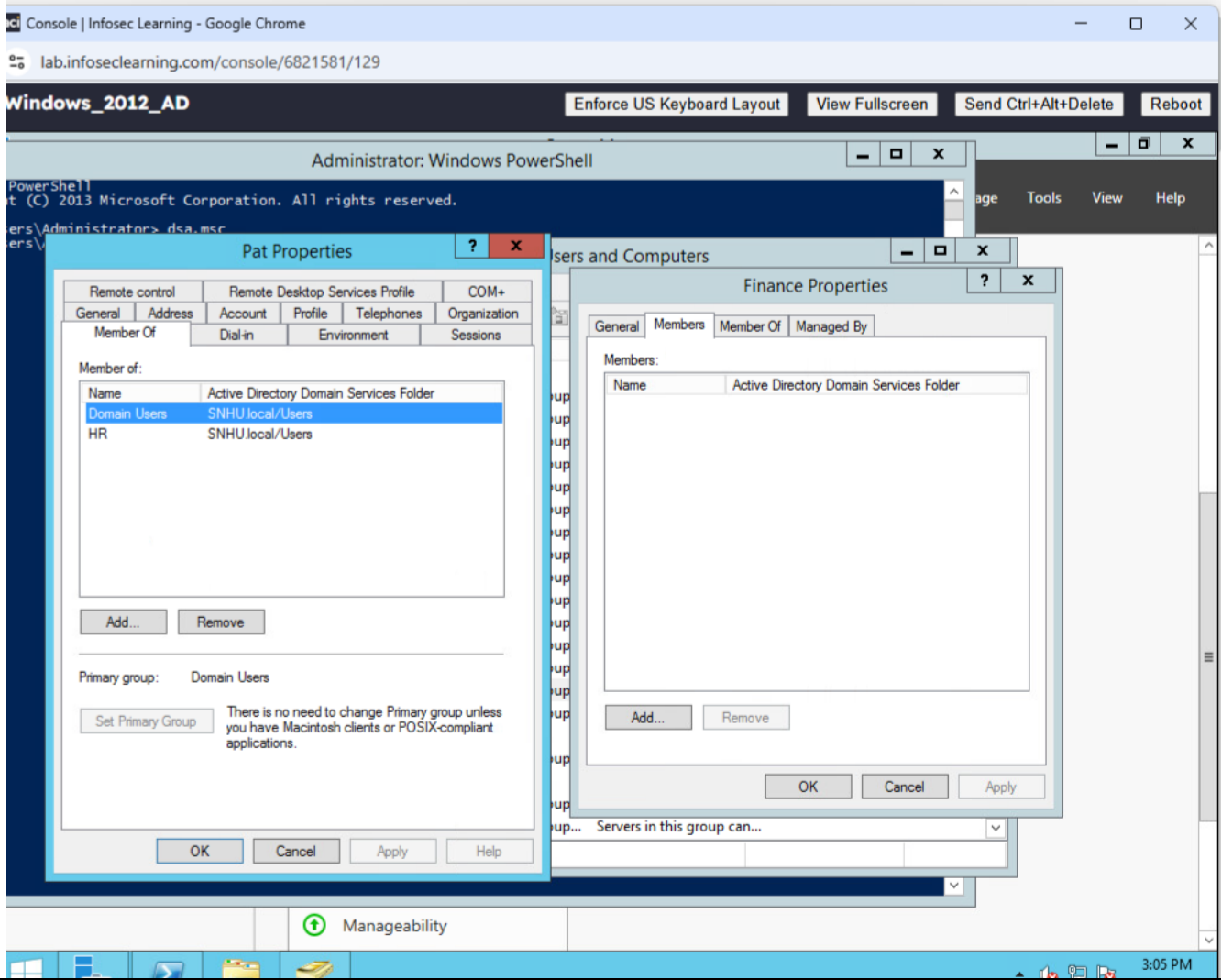
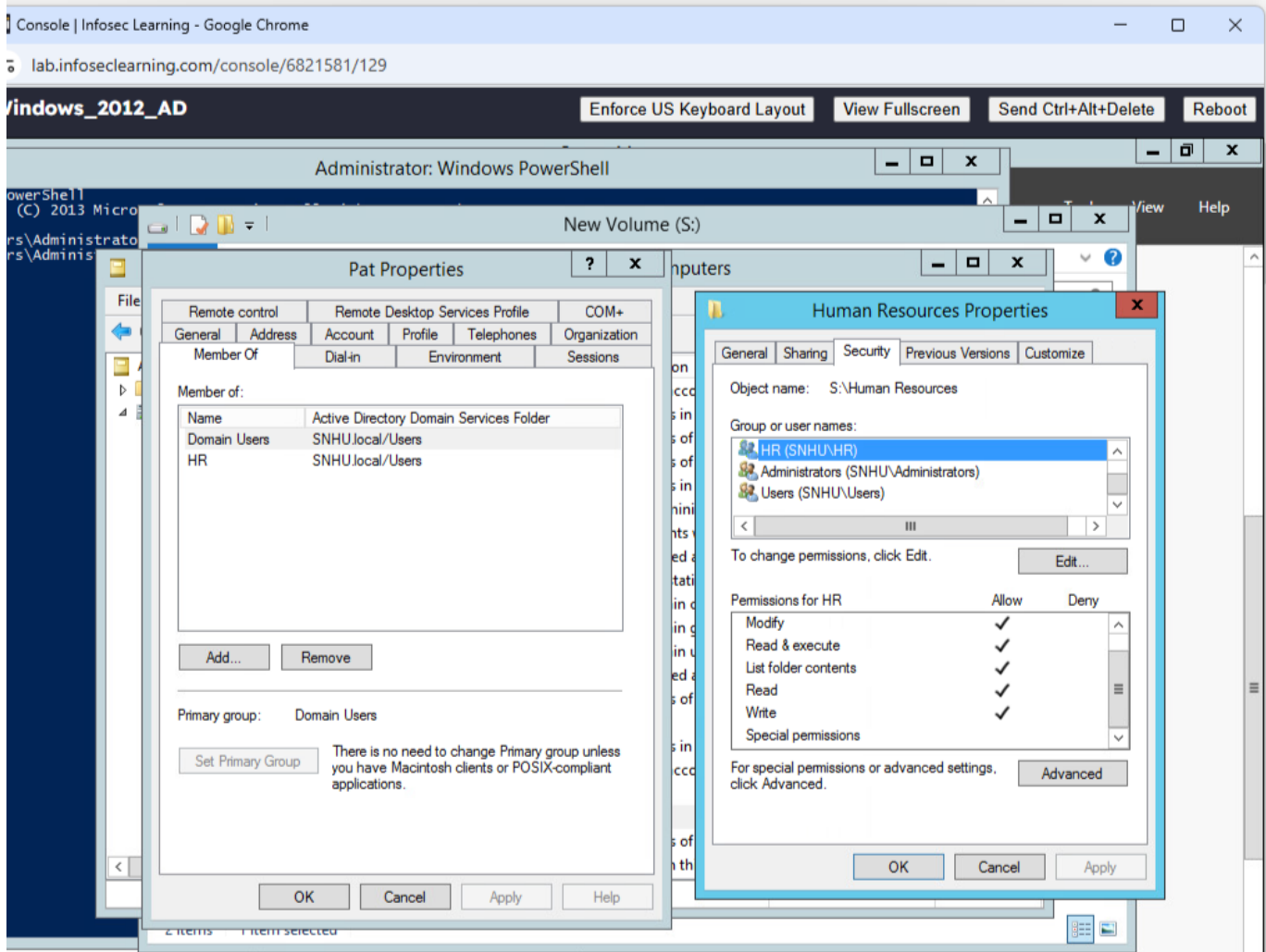
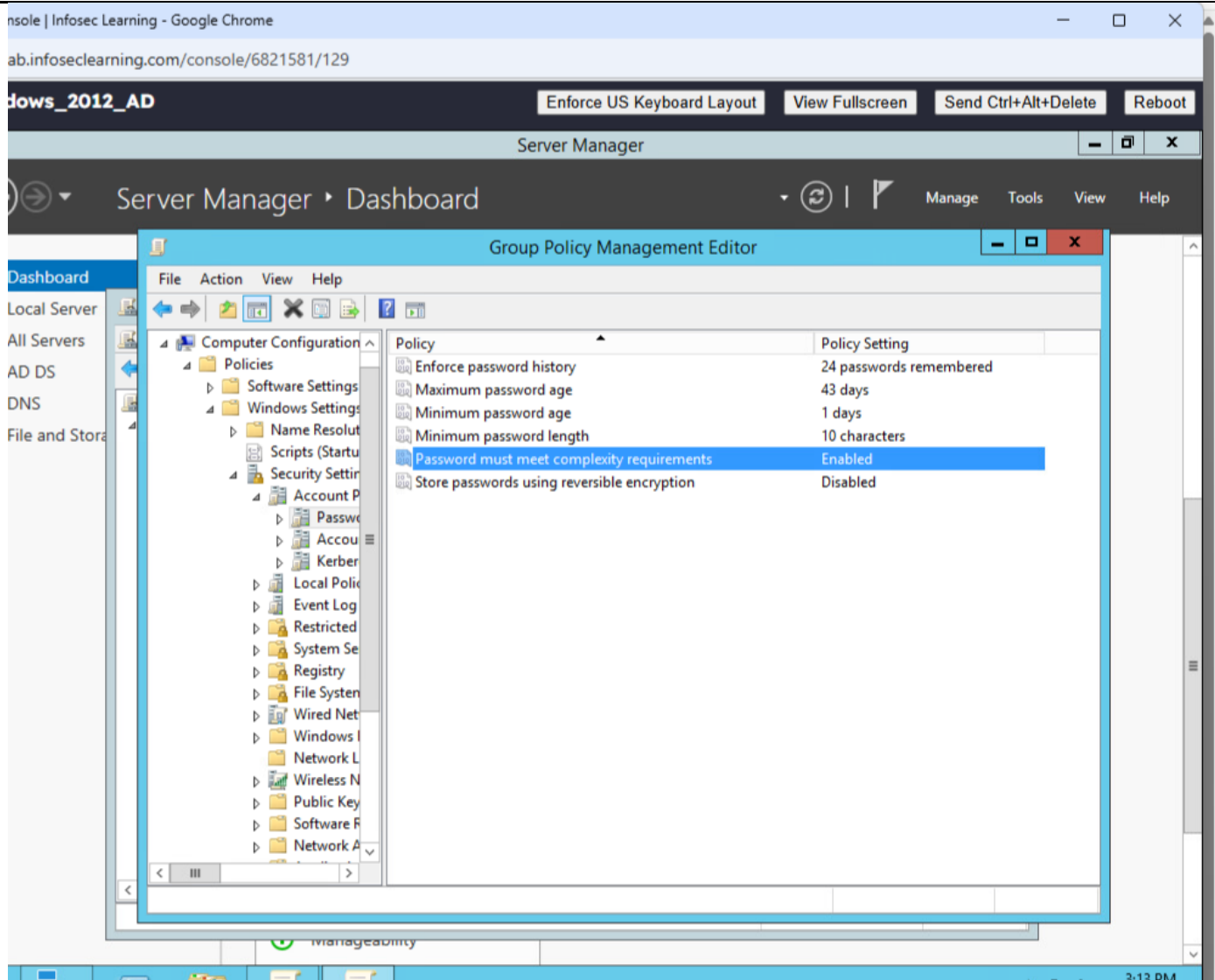


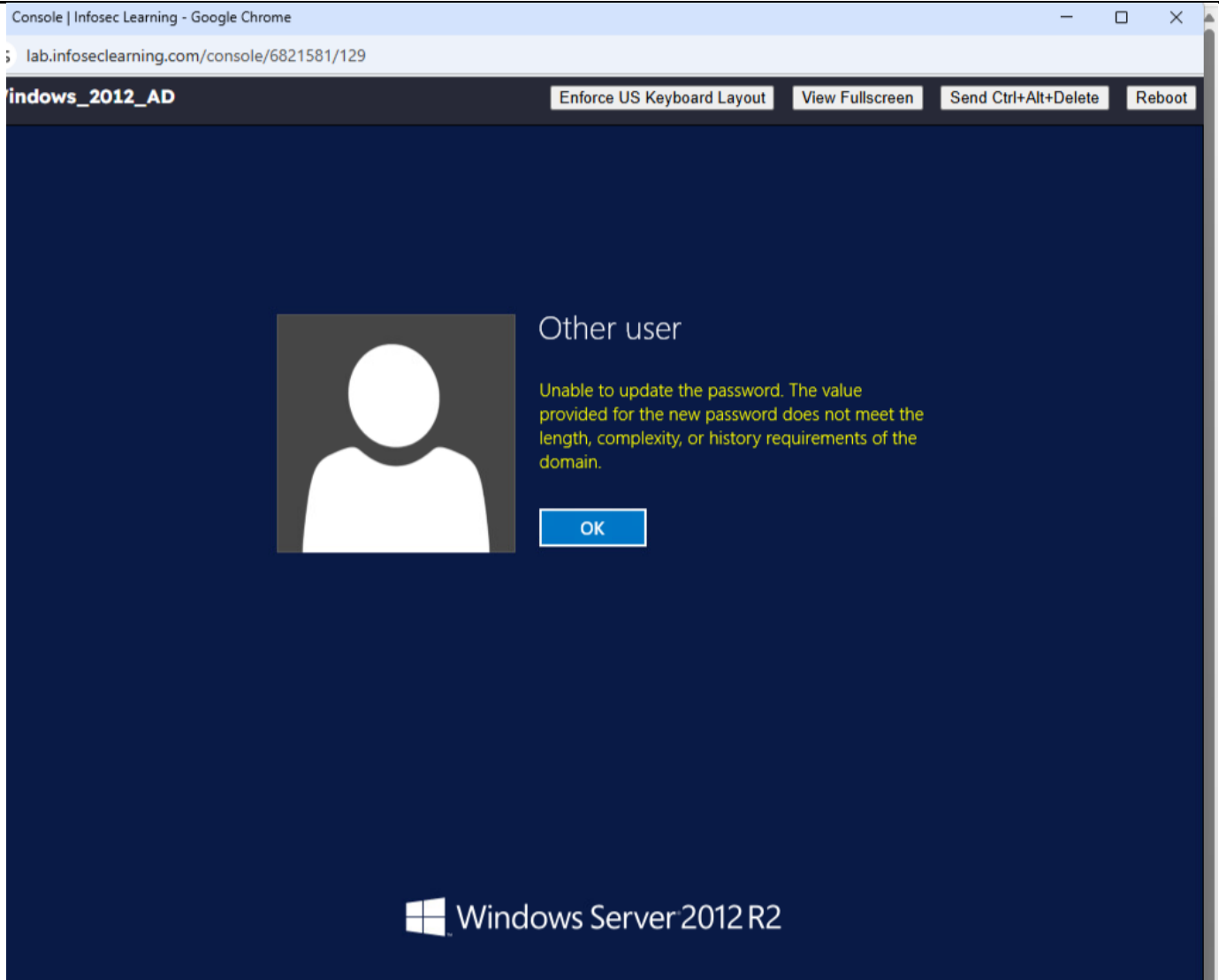
Account Modification Form

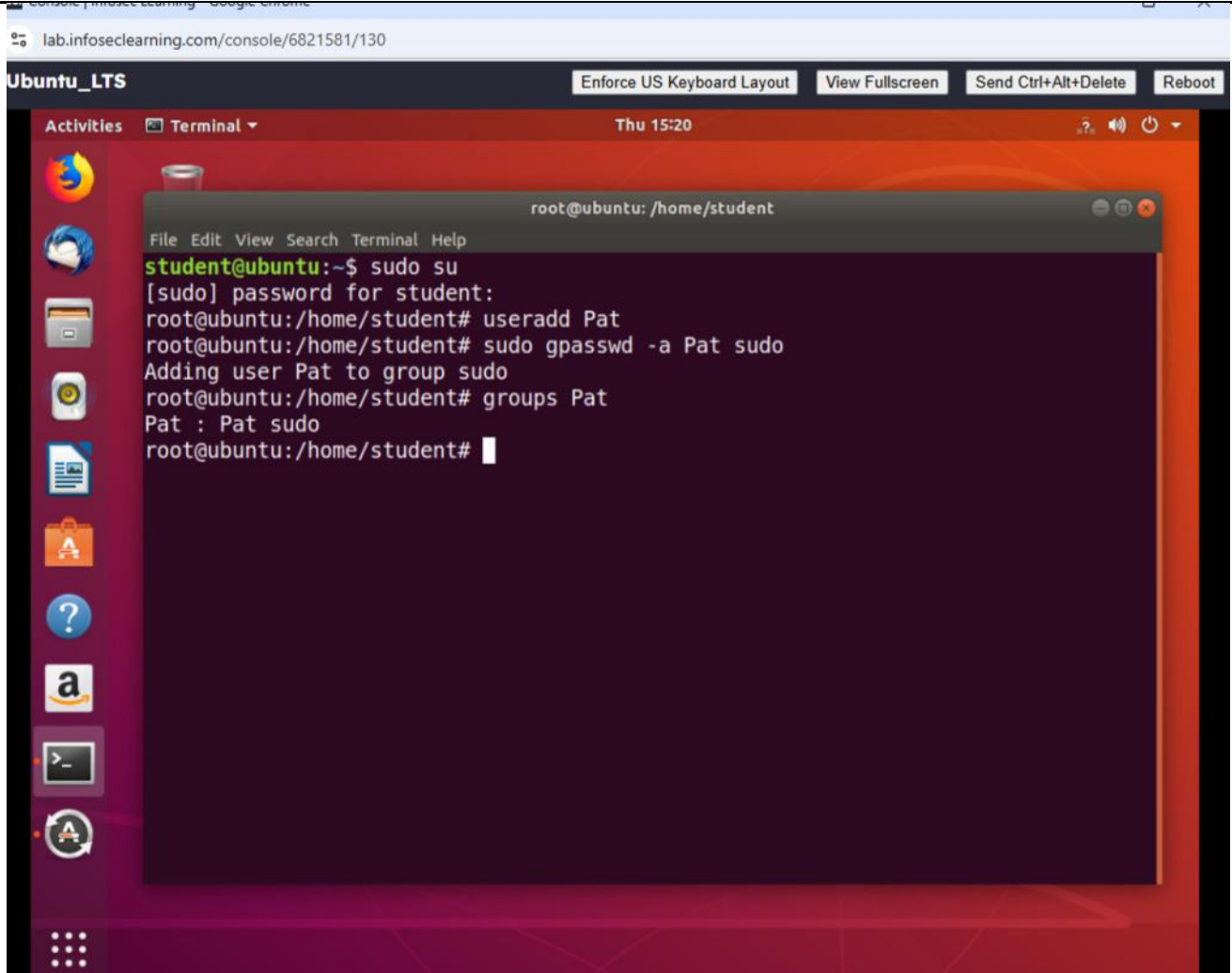
Replace the bracketed phrases in the table below with the relevant screenshots.

Systems Access	Current Permissions	Manager Approval for Modification to Access	Verification of Implementation (Filled Out by Systems Administrator)
Finance	Full control, modify, read and execute, list folder contents, read, and write	Remove Pat from all access.	 The screenshot shows a Google Chrome browser window displaying the 'lab.infoseclearning.com/console/6821581/129' page. The page title is 'Windows_2012_AD'. Below the browser window, there is a PowerShell console window titled 'Administrator: Windows PowerShell'. The PowerShell window shows the command 'dsa.msc' being executed. In the foreground, there are two overlapping windows. The first is the 'Pat Properties' window, which is a 'Group Properties' dialog box for the 'Domain Users' group. It shows the 'Members' tab with a list of members: 'Name', 'Active Directory Domain Services Folder', 'Domain Users', 'SNHU.local/Users', and 'HR', 'SNHU.local/Users'. The 'Primary group' is set to 'Domain Users'. The second window is the 'Finance Properties' window, which is also a 'Group Properties' dialog box for the 'Domain Users' group. It shows the 'Members' tab with a list of members: 'Name', 'Active Directory Domain Services Folder'. Both windows have 'Add...' and 'Remove' buttons. The background shows a Windows 2012 AD console with various tabs like 'General', 'Members', 'Member Of', and 'Managed By'. The taskbar at the bottom shows the Windows logo, a search bar, and several application icons. The system clock in the bottom right corner shows '3:05 PM'.

Systems Access	Current Permissions	Manager Approval for Modification to Access	Verification of Implementation (Filled Out by Systems Administrator)
Human resources	None	Provide Pat with all access: full control, modify, read and execute, list folder contents, read, and write.	 <p>The screenshot displays a Windows 2012 AD console interface. In the foreground, the 'Pat Properties' dialog box is open, showing the 'Member Of' tab. It lists 'Domain Users' and 'HR' as members of the 'Active Directory Domain Services Folder'. Below this, the 'Primary group' is set to 'Domain Users'. In the background, the 'Human Resources Properties' dialog box is also open, showing the 'Security' tab. It lists 'HR (SNHU\HR)', 'Administrators (SNHU\Administrators)', and 'Users (SNHU\Users)' as group or user names. The 'Permissions for HR' table shows the following permissions: Modify (checked), Read & execute (checked), List folder contents (checked), Read (checked), Write (checked), and Special permissions (unchecked). The 'Advanced' button is visible at the bottom right of the 'Human Resources Properties' dialog.</p>

Systems Access	Current Permissions	Manager Approval for Modification to Access	Verification of Implementation (Filled Out by Systems Administrator)														
GPO	User	Update to meet admin requirements for passwords.	 <p>The screenshot displays the Group Policy Management Editor interface. The left-hand navigation pane shows the hierarchy: Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies. The 'Password must meet complexity requirements' policy is selected and highlighted in blue. The right-hand pane shows the policy settings:</p> <table><thead><tr><th>Policy</th><th>Policy Setting</th></tr></thead><tbody><tr><td>Enforce password history</td><td>24 passwords remembered</td></tr><tr><td>Maximum password age</td><td>43 days</td></tr><tr><td>Minimum password age</td><td>1 days</td></tr><tr><td>Minimum password length</td><td>10 characters</td></tr><tr><td>Password must meet complexity requirements</td><td>Enabled</td></tr><tr><td>Store passwords using reversible encryption</td><td>Disabled</td></tr></tbody></table>	Policy	Policy Setting	Enforce password history	24 passwords remembered	Maximum password age	43 days	Minimum password age	1 days	Minimum password length	10 characters	Password must meet complexity requirements	Enabled	Store passwords using reversible encryption	Disabled
Policy	Policy Setting																
Enforce password history	24 passwords remembered																
Maximum password age	43 days																
Minimum password age	1 days																
Minimum password length	10 characters																
Password must meet complexity requirements	Enabled																
Store passwords using reversible encryption	Disabled																

Systems Access	Current Permissions	Manager Approval for Modification to Access	Verification of Implementation (Filled Out by Systems Administrator)
GPO	n/a	Test Pat's account for the logon error displayed after you update the password requirements.	 <p>The screenshot shows a Google Chrome browser window titled 'Console Infosec Learning - Google Chrome' with the address bar displaying 'lab.infoseclearning.com/console/6821581/129'. The main content area is a dark blue Windows Server 2012 R2 console window titled 'indows_2012_AD'. At the top of the console window, there are four buttons: 'Enforce US Keyboard Layout', 'View Fullscreen', 'Send Ctrl+Alt+Delete', and 'Reboot'. The console displays a message for 'Other user' with a white silhouette icon of a person. The message text reads: 'Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirements of the domain.' Below the message is a blue 'OK' button. At the bottom of the console window, the Windows logo and 'Windows Server 2012 R2' are visible.</p>

Systems Access	Current Permissions	Manager Approval for Modification to Access	Verification of Implementation (Filled Out by Systems Administrator)
Linux server	None	Create HR admin user for Pat.	 <p>The screenshot shows a terminal window titled 'root@ubuntu: /home/student'. The user 'student' has executed the command 'sudo su' and entered the password for 'student'. The root user has then executed the following commands: 'useradd Pat', 'sudo gpasswd -a Pat sudo', and 'groups Pat'. The output of the last command shows that 'Pat' is a member of the 'sudo' group.</p> <pre> root@ubuntu: /home/student File Edit View Search Terminal Help student@ubuntu:~\$ sudo su [sudo] password for student: root@ubuntu:/home/student# useradd Pat root@ubuntu:/home/student# sudo gpasswd -a Pat sudo Adding user Pat to group sudo root@ubuntu:/home/student# groups Pat Pat : Pat sudo root@ubuntu:/home/student# </pre>