KURUKULASOORIYA KVR **200332X**

CS 3400 CYBER SECURITY PROJECT

Week Six at Pandora Company Limited: Bridging the Islands of Systems Chaos

It was identified that decentralized PC/user management in Pandora Company Ltd creates many inefficiencies and security risks that could lead to financial losses, data breaches and compliance violations. To address this issue, a comprehensive analysis of the current system, possible areas of improvement, and suggestions to rectify them were reviewed and drafted into the report. This report primarily contains 3 sections including Unified Management Exploration, Advantages and benefit Analysis, and Recommendation Action Plan to migrate the current chaotic system to a secure and efficient system.

1) Unified Management Exploration

There are so many challenges and risks that could be identified in Pandora Company Ltd due to its decentralized PC management.

1. **Inconsistent User Policies, Software Installations, and Security Configurations:** In a decentralized PC management system, where each PC is managed individually, security policies can vary from PC to PC, or even be nonexistent. This inconsistency can lead to vulnerabilities and security breaches because an attacker may exploit a known vulnerability or configuration error to gain access and then compromise the system.
2. **Use of Weak Passwords:** Employees using weak passwords like "1234" creates a significant security risk since it is commonly used, it leaves the system open for unauthorized access. Often employees may be more likely to use weak passwords if they do not need to adhere to a central password policy. Especially in a decentralized system, enforcing password policies is challenging and it will leave the PCs getting unauthorized access and vulnerable to attack.
3. **Inconsistencies in Deploying Updates:** It can be difficult to deploy updates uniformly across all PCs in a decentralized environment and easily expose the company system to known vulnerabilities.
4. **Inconsistent Access Control Restriction:** Granting, managing, revoking, and auditing access permissions become very complex in a decentralized system. Thus, it is more time-consuming and requires more effort but still, there is a big chance that due to human error, the system data may lead to unauthorized access.
5. **Possible malware and phishing scams** [1]**:** Since it is difficult to keep all PCs patched and enforce consistent security policies, employees may use the PCs at their convenience (e.g. download any attachments in emails, plug any kind of external device into the PC, disable

firewalls and etc.) and leave them open for malware to get installed or get trapped to phishing attacks.

To address such issues in Pandora Company Ltd, there are 2 commonly used enterprise-level solutions that could be identified as

- **MS Active Directory** which is a directory service that provides a centralized approach to managing user accounts, computers, and other resources in a Windows domain network &
- **UEM** (**Unified Endpoint Management**) **Tool** which provides a single stage of control for managing all devices in the network regardless of their type or operating system.[2]

Since the Pandora Company Network is not totally run in the Windows Domain (e.g. Database Server runs on Rockey Linux), **Implementation of a UEM would be the recommended solution** which would be more complex with some additional features contained than AD but in the meantime would be more expensive. [2]

The Suggested Solution: Implement a Unified Endpoint Management

UEM is a solution for managing all types of endpoints from a single unified platform. This provides a wide range of coverage of devices to get connected allowing desktop/ laptop computers, mobile devices, and also IOT devices. This is usually used to manage user accounts, software installation and patch management, security configurations, and other settings over all the devices connected. [3]

"The most popular UEM solutions in the market are **VMWare Workspace ONE, Microsoft Intune, BlackBerry UEM, and MobileIron**." **The choice of the most suitable UEM solution for Pandora Company Ltd would totally depend upon the significance of its need, technology stack, and budget considerations.**[4]

A typical UEM Platform usually contains several components to provide a value-added service in Unified PC Management:

- **Device Management:** UEM enables connecting devices to the service via a mobile device management (MDM) protocol which allows the service to interact remotely with a device, sending it configurations, commands, and queries. This implies that devices do not need to be on a corporate network or VPN to be managed by a UEM solution. Plus it also provides device management services like configuring encryption, setting passcode policies, managing their OS and app patches, location tracking, remote control, and much more. [3]
- **OS and Device Support:** UEM supports and manages a wide range of devices including mobile devices, desktops, laptops, wearables, and ruggedized devices plus virtual desktops with different types of Operating systems while helping the company to improve the security, manageability, and compliance of their devices. [3]

- **Identity and Access Control:** UEM and IAM can work together to make sure that only authorized devices and users can access corporate resources. UEM can also provide additional information about devices to IAM systems, which can help IAM systems make better decisions about access.[3]
- **Security:** UEM solutions provide additional security features, such as device integrity monitoring, network security, mobile app reputation service, and phishing prevention. MTD (Mobile Threat Defense) deployments that are already put in place can benefit greatly from UEM integration.[3]
- **Enables the concept of BYOD (Bring Your Own Device) & Privacy:** UEM platforms can apply corporate policies to specific apps and data on BYOD devices without affecting personal apps and data. This also provides facilities to limit administrator roles, thus the admins cannot see or do anything to affect the personal side of a device. [3]

2) Advantages & Benefits Analysis

In contrast with decentralized PC management, switching to a single unified user/system management system has many benefits of both immediate and far-reaching gains.

2.1) Immediate Gains from Centralized Mgt

1. **Enables Centralized Administration:** Unified user/system management systems centralize control of access, permissions, and configurations, simplifying and streamlining user and system administration. Thus, all access control granting, modification, and revoking plus setting configurations and patching all PCs can be done using a single interface with one administrator control. [5]

2. **Saves the cost:** Since the distributed control of resources has been eliminated now, the company can benefit from reduced labor costs, multiple license purchases, maintenance, and support costs.[5]

3. **Improved level of Security:** Unified systems comply with single and consistent security policies and system-wide access control across all the devices and users connected to it. Thus, it reduces the risk of unauthorized access, security breaches, or known vulnerability exploitations. [5][6]

4. **Increased efficiency:** Since there is no longer a need to do repetitive tasks across all the devices connected such as patching, configuration setting, and managing user access for each device, the system administration becomes faster and easier to manage while reducing the inherited risk of possible human error. [5]

5. **Increased simplicity:** Simplicity is considered to be a very important aspect of a system with good security. Unified system management enables simplicity by providing a single interface for managing all users and systems while eliminating the need for system administrators to learn and use multiple tools. Thus, the one single interface with all necessary options to secure and manage all the system-wide tasks will ensure the benefits of not being too complex. [5]

2.2) Indirect Gains from Centralized Mgt

1. **Improved User Experience:** Unified system management allows users to focus on their work, rather than worrying about managing or securing their devices. Often it's tasks of provisioning, configuring, and managing devices are automated and therefore it frees up the administrative effort and time of the users.[6] Plus, it also provides features like remote access, mobile device management, and application virtualization which allows the users with the flexibility to access their work resources from anywhere. [7]

2. **Reduced issues of Compliance:** Achieving compliance with regulations and standards is made easier with a unified system that enforces uniform policies and records user actions. Though the compliance standards change, the whole system could remain up to date with the help of Unified System management solutions.[6]

3. **Enabled BYOD:** Since BYOD which is a very useful policy that allows employees to bring and use their own personal devices for work-related tasks, could be easily implemented and securely managed through unified System management, the following indirect benefits could be obtained.
   - **Improved Collaboration:** Employees using their personal devices for work often tend to feel more empowered and productive.[7] Together with unified connectivity, teams collaborate better by having the same access to shared resources, which encourages teamwork and sparks innovation.
   - **Scalability: Since adding more and more devices/ access permission** becomes easier, as the company grows, a unified system could scale with it more efficiently while ensuring the same level of security.[7]
   - **Support for Remote and hybrid work: BYOD enables** providing seamless access to resources for both on-site and remote employees to become very easy and it will help to increase both workforce flexibility and job satisfaction. [7]

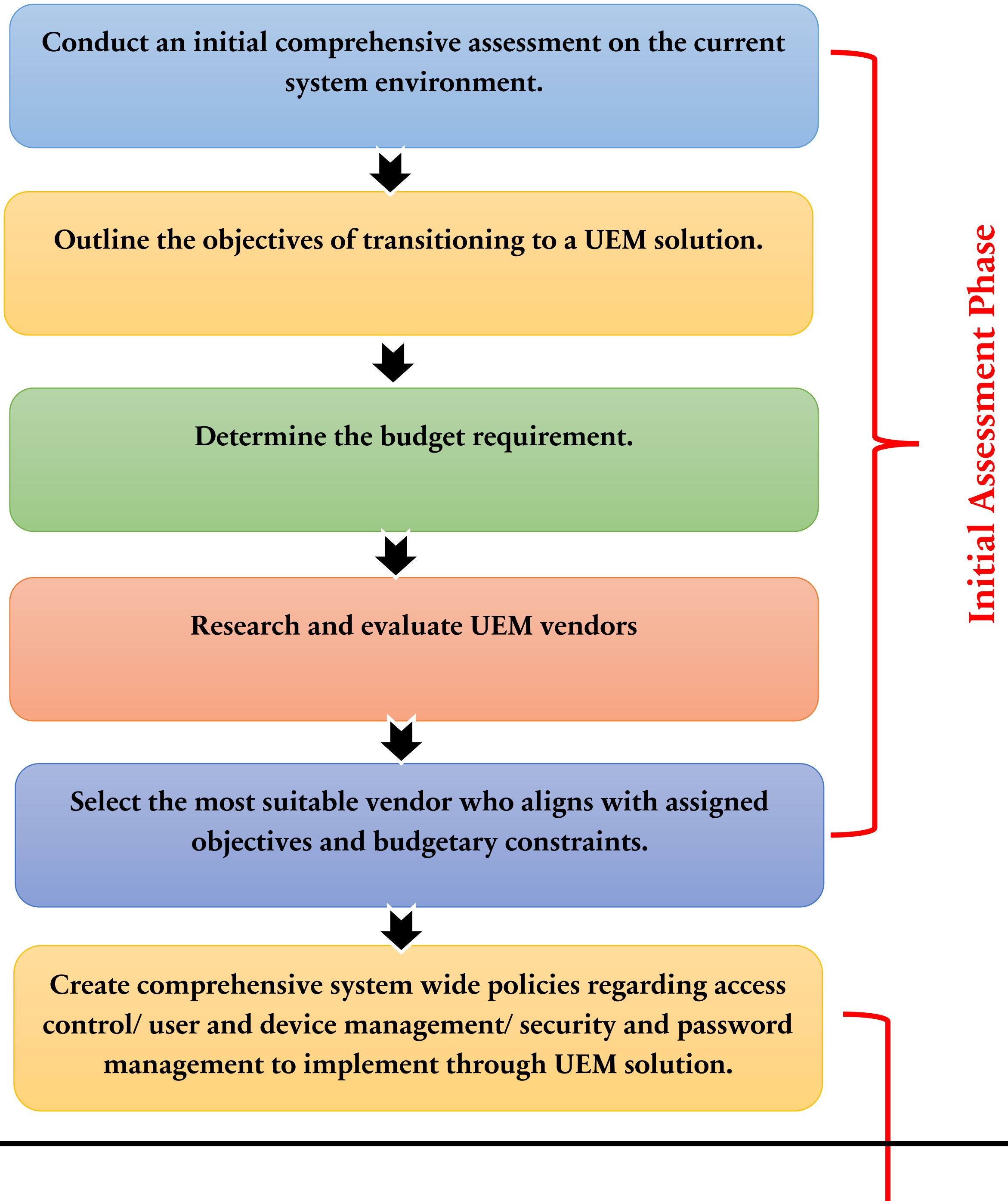
4. **Provide Performance Statistics to improve system-wide quality:** Since a Unified system, management could collect all user and system data in one spot in real-time, [6] organizations

can use data analysis and reporting tools to learn about how users behave in terms of accessing and resource utilization, how systems are used, and security trends. This helps in making better decisions and finding areas to improve.

3) Recommendation Report

The pivotal measure to address the ongoing issue would be shifting from Pandora Company Limited's current fragmented PC management system to a centralized Unified Endpoint Management (UEM) solution. By adhering to the following suggested action plan, the company can effectively reduce risks and benefit from the numerous advantages of a unified user/system management approach.

Migration to UEM: Action Plan [8][9]



Conduct an initial comprehensive assessment on the current system environment.

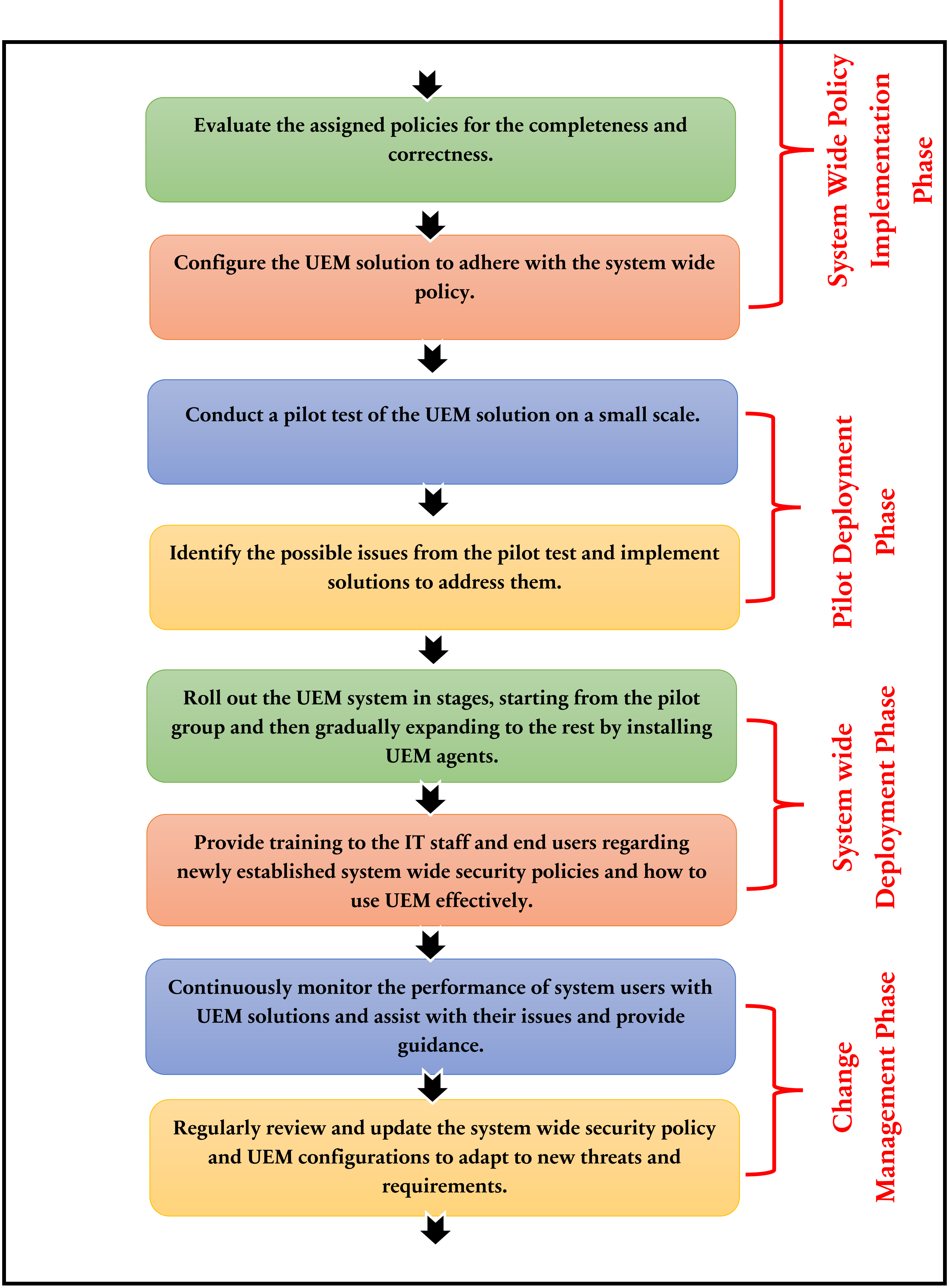
Outline the objectives of transitioning to a UEM solution.

Determine the budget requirement.

Research and evaluate UEM vendors

Select the most suitable vendor who aligns with assigned objectives and budgetary constraints.

Create comprehensive system wide policies regarding access control/ user and device management/ security and password management to implement through UEM solution.



Evaluate the assigned policies for the completeness and correctness.

Configure the UEM solution to adhere with the system wide policy.

Conduct a pilot test of the UEM solution on a small scale.

Identify the possible issues from the pilot test and implement solutions to address them.

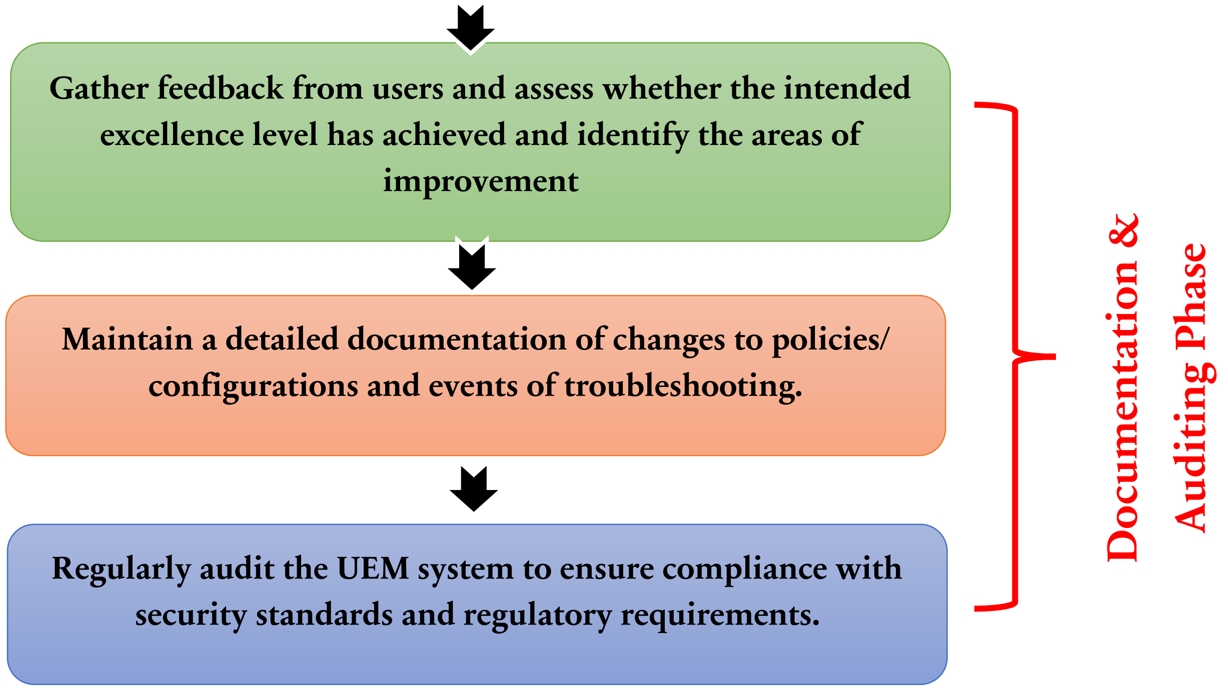
Roll out the UEM system in stages, starting from the pilot group and then gradually expanding to the rest by installing UEM agents.

Provide training to the IT staff and end users regarding newly established system wide security policies and how to use UEM effectively.

Continuously monitor the performance of system users with UEM solutions and assist with their issues and provide guidance.

Regularly review and update the system wide security policy and UEM configurations to adapt to new threats and requirements.

System Wide Policy Implementation Phase
Pilot Deployment Phase
System wide Deployment Phase
Change Management Phase



Gather feedback from users and assess whether the intended excellence level has achieved and identify the areas of improvement

Maintain a detailed documentation of changes to policies/ configurations and events of troubleshooting.

Regularly audit the UEM system to ensure compliance with security standards and regulatory requirements.

Migrating to a UEM solution would not be an easy task because it involves a significant transformation of the existing IT infrastructure, which may encounter resistance from employees and require adjustments to established workflows. [9] However, by adhering to a well-thought-out plan with the right strategy, the company can systematically address these challenges, minimize disruptions, and ultimately achieve a successful transition.[8]

References

[1] Suzannah Hastings on Faronics, "Top 4 security challenges while working with decentralized workspaces", [2020 November 11], Available at: https://www.faronics.com/news/blog/top-4-security-challenges-while-working-with-decentralized-workspaces

[2] Brendon Baxter on Hexnode, "UEM vs Group Policy Object: Why UEMs have an edge over GPOs in Windows Device Management", [2023 May 19], Available at: https://www.hexnode.com/blogs/uem-vs-group-policy-object/

[3] Nick Schmiedicker on TechTarget, "What is unified endpoint management (UEM)? A Complete Guide", [2023 March], Available at: https://www.techtarget.com/searchenterprisedesktop/definition/unified-endpoint-management-UEM

[4] Daniel Hein on Solutions Review, "The 13 best unified endpoint management solutions for 2021", [2021 January 14], Available at: https://solutionsreview.com/mobile-device-management/best-unified-endpoint-management-solutions/

[5] Gagan S on Linkedin, Why enterprises should consider unified endpoint management and specifically Microsoft Intune", [2023 July 01], Available at: https://www.linkedin.com/pulse/why-enterprises-should-consider-unified-endpoint-management-gagan-s

[6] Lauren Ballejos on ninjaOne, "Benefits of Unified Endpoint Management for Business", [2022 November 21], Available at: https://www.ninjaone.com/blog/benefits-of-unified-endpoint-management-for-businesses/

[7] vmware, "What is bring your own device?", Available at: https://www.vmware.com/topics/glossary/content/bring-your-own-device-byod.html

[8] White Papers on hexnode, "UEM Migration Handbook: An IT admin's guide for effective migration", Available at: https://www.hexnode.com/resources/white-papers/uem-migration-handbook-an-it-admins-guide-for-effective-migration/

[9] Unisys Corporation, "Four Obstacles to UEM Migration and How to overcome Them", [2022 October 27], Available at:https://www.unisys.com/blog-post/dws/four-obstacles-to-uem-migration-and-how-to-overcome-them/