ISM-1687: Privileged operating environments are not virtualised within unprivileged operating environments.

**Explanation of ISM-1687**

This control is fundamentally about **separation of concerns and preventing escalation of privilege**.

* **Privileged Operating Environment:** Think of this as your "kingdom" where highly sensitive operations occur. This could be:
  + A hypervisor (like VMware ESXi, Microsoft Hyper-V, KVM) managing virtual machines.
  + A Security Information and Event Management (SIEM) system.
  + An identity management system (e.g., Active Directory Domain Controllers, FreeIPA).
  + A Certificate Authority (CA).
  + Critical network devices (firewalls, routers, core switches).
  + Systems storing highly classified or sensitive data. These environments often have elevated permissions, direct access to hardware or core network functions, and are critical for the overall security posture.
* **Unprivileged Operating Environment:** This is your "common land" where every day, less sensitive operations take place. Examples include:
  + User workstations.
  + Standard application servers (web servers, file servers, databases not holding highly sensitive data).
  + Development or test environments.
  + Guest virtual machines running typical business applications.
* **"Not virtualised within":** This is the core of the control. It means you should *not* run a privileged operating environment as a guest virtual machine *inside* an unprivileged operating environment.

**Why is this important?**

Imagine you have a highly secure vault (privileged environment) and you decide to put a mini-vault (a virtualized privileged environment) *inside* a regular office cubicle (unprivileged environment). If someone compromises the cubicle, they now have a direct pathway to compromise your mini-vault, which in turn could give them access to your main, highly secure vault.

In technical terms, if a privileged environment (e.g., a domain controller) is virtualized on an unprivileged host (e.g., a standard Windows server also running other non-critical applications), a compromise of the *unprivileged host operating system* could directly lead to:

1. **Hypervisor compromise:** If the unprivileged host *is* the hypervisor for the privileged VM, a compromise of the host could give an attacker control over the privileged VM.
2. **VM Escape:** While difficult, vulnerabilities exist that allow an attacker to "escape" from a guest VM to the underlying hypervisor. If your privileged environment is a guest on an unprivileged hypervisor, a successful VM escape from another unprivileged guest on that *same* hypervisor could compromise your privileged environment.
3. **Resource sharing risks:** Unprivileged environments might have broader network access, less stringent patching cycles, or more users with local administrative rights, all of which increase the attack surface for the co-located privileged environment.
4. **Supply chain attacks/software vulnerabilities:** Software running in unprivileged environments might introduce vulnerabilities that could be exploited to affect the co-located privileged environment.
5. **Simplified lateral movement:** If an attacker breaches the unprivileged environment, they are already on the same physical or virtual hardware as the privileged environment, making lateral movement easier.

Essentially, this control aims to create a strong logical and often physical separation between environments with different trust levels to minimize the impact of a compromise in a lower-trust environment.

**Controls and Evidence to Collect for Verification**

To verify compliance with ISM-1687, you'd want to gather evidence that demonstrates the isolation and appropriate placement of privileged environments. Here's a breakdown:

**1. Architectural Documentation & Design Reviews**

**Controls:**

* **Enterprise Architecture Diagrams:** Up-to-date diagrams illustrating the logical and physical placement of all systems, clearly identifying privileged and unprivileged environments.
* **Virtualization Strategy/Policy:** Documentation outlining the organization's approach to virtualization, explicitly stating that privileged environments will not be virtualized within unprivileged ones.
* **System Design Documents:** For specific privileged systems, design documents should show how they are deployed and hosted.
* **Network Segmentation Diagrams:** Show how privileged environments are segmented from unprivileged ones at the network level.

**Evidence to Collect:**

* **Interview Architects/Engineers:** Discuss their understanding and implementation of this control.
* **Review Architectural Diagrams:** Visually confirm the separation. Look for dedicated hypervisor clusters for privileged VMs, or physical segregation for highly critical systems.
* **Review Virtualization Policies:** Check for specific clauses addressing the placement of privileged VMs.
* **Review System Design Specifications:** For a sample of critical systems, verify their hosting environment.

**2. Inventory and Asset Management**

**Controls:**

* **Comprehensive Asset Inventory:** A complete and accurate list of all IT assets, including physical servers, virtual machines, and their designated function (privileged/unprivileged).
* **Configuration Management Database (CMDB):** If available, the CMDB should accurately reflect the relationships between VMs and their hosts.

**Evidence to Collect:**

* **Extract Asset Inventory Reports:** Filter for virtual machines identified as "privileged" (e.g., Domain Controllers, SIEMs, CAs).
* **Cross-Reference with Hypervisor Inventory:** Compare the list of privileged VMs from the asset inventory with the actual VMs running on hypervisors.
* **Review CMDB Records:** If a CMDB is used, verify that relationships between privileged VMs and their hosts are correctly recorded.

**3. Virtualization Platform Configuration & Management**

**Controls:**

* **Dedicated Hypervisor Clusters:** Privileged VMs should ideally reside on dedicated hypervisor clusters that *only* host privileged workloads.
* **Hypervisor Hardening:** The hypervisors themselves (that host privileged VMs) should be rigorously hardened according to security best practices (e.g., CIS benchmarks).
* **Role-Based Access Control (RBAC) on Hypervisors:** Strict RBAC should be enforced on hypervisors to limit who can access and manage privileged VMs.
* **Network Configuration on Hypervisors:** Ensure that network adapters used by privileged VMs are on segmented networks.

**Evidence to Collect:**

* **Hypervisor Configuration Snapshots/Exports:**
  + **VM placement:** Show which VMs are running on which hosts. Look for privileged VMs on dedicated clusters or hosts.
  + **Network settings:** Verify network segmentation for privileged VM networks.
  + **User/Group permissions:** Check RBAC for hypervisor management interfaces.
* **Logs from Hypervisor Management:** Look for activity logs indicating VM deployment, migration, or configuration changes to ensure adherence to policy.
* **Interview Virtualization Administrators:** Ask about their procedures for deploying and managing privileged VMs.
* **Review Hypervisor Hardening Checklists/Reports:** Verify that the underlying hypervisors for privileged VMs are appropriately secured.

**4. Network Security & Segmentation**

**Controls:**

* **Network Segregation:** Privileged operating environments (both physical and virtual) should be logically and physically separated from unprivileged environments using firewalls, VLANs, or other network segmentation techniques.
* **Traffic Filtering Rules:** Strict firewall rules should be in place to limit communication between privileged and unprivileged networks.

**Evidence to Collect:**

* **Firewall Configuration Reviews:** Examine firewall rules to confirm that privileged network segments are isolated and that communication is restricted.
* **Network Diagrams:** Verify that network segmentation is clearly depicted and aligns with the principle of separation.
* **VLAN Configuration:** Review VLAN configurations on switches to ensure proper segregation.
* **Packet Captures (if necessary and approved):** To confirm traffic flow restrictions between segments.

**5. Access Control and Identity Management**

**Controls:**

* **Least Privilege:** Access to privileged operating environments and the hypervisors hosting them should be strictly controlled based on the principle of least privilege.
* **Multi-Factor Authentication (MFA):** MFA should be required for access to privileged environments and their management interfaces.

**Evidence to Collect:**

* **User Access Reports:** Generate reports showing who has access to privileged systems and their underlying hypervisors.
* **Review Access Control Lists (ACLs):** On privileged systems and hypervisors.
* **MFA Configuration:** Confirm MFA is enabled for relevant accounts.

**6. Incident Response & Monitoring**

**Controls:**

* **Logging and Monitoring:** Robust logging and monitoring should be in place for both privileged environments and the hypervisors hosting them, with alerts for suspicious activity.
* **Incident Response Playbooks:** Procedures for responding to security incidents involving privileged environments should be well-defined.

**Evidence to Collect:**

* **Review SIEM/Log Management Data:** Look for logs related to privileged VM creation, migration, or access, and ensure they are coming from the correct, segregated sources.
* **Review Incident Response Procedures:** Confirm that the response plans align with the criticality of privileged environments.

**Summary of Verification Approach:**

Your verification strategy should involve a combination of:

* **Document Review:** Policies, architecture diagrams, asset inventories, configuration documents.
* **Technical Configuration Review:** Directly examining hypervisor configurations, network device configurations, and system settings.
* **Interviews:** Talking to system administrators, network engineers, and security personnel to understand their processes and knowledge.
* **Log Analysis:** Reviewing security logs for anomalies or non-compliant activities.

By collecting and analysing this evidence, you can form a strong opinion on whether the organization is effectively complying with ISM-1687 and protecting its most critical operating environments. Remember to focus on the *why* behind the control – preventing unauthorized access and privilege escalation – throughout your assessment.