SC.L2-3.13.3

System & Communications Protection

Role Separation

"Separate user functionality from system management functionality."

Objectives

[a]
User functionality is identified.

[b]
System management functionality is identified.

[c]
User functionality is separated from system management functionality.

Key Discussion Points

Two Account Types:
Standard user accounts for daily work; privileged accounts for admin tasks — using one account for both defeats the separation this control requires.

Physical or Logical:
Separation can be different machines, different VMs, different network addresses, or jump servers — any method that prevents user activity from reaching admin interfaces qualifies.

Admins Use User Accounts:
System administrators must perform their own daily user tasks — email, browsing, meetings — from their standard user account, not their privileged account.

Reduces Attack Surface:
If an attacker compromises a user account, lack of separation allows immediate escalation to admin access — separation breaks that escalation path.

Assessment Methods

EXAMINE

System and communications protection policy; procedures addressing application partitioning; system design documentation; system configuration settings; system security plan; system audit logs.

INTERVIEW

System or network administrators; personnel with information security responsibilities; system developer.

TEST

Separation of user functionality from system management functionality.

SC.L2-3.13.3

SYSTEM & COMMS PROTECTION — Role Separation

Plain English

What this control is really saying:

A system administrator who uses a single account for both daily email and server administration is an insider threat waiting to happen — and a privileged target for attackers. This control requires that the functions users perform and the functions admins perform be separated, so administrative access cannot be reached through a compromised user account.

How it is used:

- System administrators have two accounts: a standard user account for email and daily work, and a separate privileged account used only for administrative tasks.
- Administrative access to servers and network devices is only possible from a dedicated jump server — admin functions cannot be performed from general user workstations.
- CUI application interfaces do not expose administrative functions to standard users — database admin consoles, server management tools, and configuration interfaces are separately authenticated and access-controlled.
- User and admin accounts are documented in the SSP — account types, access levels, and the separation mechanism are all described.

Real World Example

The Scenario

Acme Defense's IT admin has one Windows account. He uses it for email, web browsing, Teams meetings, and managing all servers and network devices. When he needs to administer a server, he simply runs the management console from his everyday user account.

What the assessor finds

A phishing email tricks the IT admin into clicking a malicious link. The attacker gains control of his user session — and with it, full administrative access to all servers, network devices, and CUI systems. No separation existed to limit what an attacker could do through a compromised user account.

SPRS Score Impact

3.13.3 carries a point value of 1. The absence of role separation means that any compromise of a user account is also a compromise of administrative access — it collapses the distinction between user and privileged access entirely.

What Good Looks Like

User and admin functions identified and documented, separate accounts for user and admin activity, admin functions only accessible via privileged accounts from controlled access paths, jump server or equivalent separation in place, separation documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ Single account for all tasks

System administrators use one account for both daily user activity and system management — compromising the email account also compromises the admin account.

✗ No jump server

Admin functions are performed directly from user workstations — there is no logical or physical separation between user and admin access paths.

✗ Admin tools accessible to users

Database management consoles and server configuration tools are installed on user workstations — standard users can access them without restriction.

✗ Separation not documented

Different accounts may exist but the separation architecture is not documented in the SSP — assessors cannot verify the separation is enforced.

✗ Admins do user work on admin account

System administrators use their privileged accounts for day-to-day user tasks — the admin account is exposed to the same risks as a user account.