GRC Fokusgruppmöte

SAPSA IMPULS 2022-11-08

Governance, Risk and Compliance (GRC)

Meetings

- 2022-01-19
- 2022-03-18
- VårIMPULS
- 2022-06-03
- 2022-08-26
- 2022-10-07
- 2022-11-07 IMPULS (Monday – Tuesday)
- **2022-11-08 IMPULS + fokusgruppsmöte**

How to manage Segregation of Duty and Critical access risks

1. Verify and classify risk by Risk Owner
2. Exclude false positive hits
3. Check if the process could be changed to avoid the risk
4. Ensure task roles (functional) do not have built in SoD risks
5. Close not used accounts(revoke access and delete)
6. Revoke access not used last 13 months
7. Make Job roles (Composite roles) SoD risk free by move critical access to Business role
8. Make Business roles (GRC roles) SoD risk free by move critical access to User
9. Reassign critical role or accept the risk per user
10. Define compensating control to mitigate accepted risk
    a) Identify most critical used transactions and define how to perform the control
    b) Identify most common scenarios and define how to perform the control
    c) Whitelist users (3- 12 months) considered as low risk
    d) Allocate performer and start the control (WF with or without approval)

Lessons learned

- Identify stake holders
- Don’t use Fire Fighter to hide risks
- Introduce Risk Managers as a filter to avoid new risks
- Perform Roel Content Review to have appropriate roles
- Perform User Access Reaffirm to minimize risk exposure

GRC Fokusgruppmöte

SAPSA IMPULS 2022-11-08

Governance, Risk and Compliance (GRC)