Del 3 – Segregation of Duties

IGDLA-implementation i Active Directory
GreenTyre Recycling AB

Datum: 2026-02-28

Upprättad av: Julian Rieger – IT-säkerhetskonsult

Kurs: IAM – Identity and Access Management

Domän: mylab.local (Windows Server 2019)

Klient: Windows 11 (domänansluten)

1. Inledning

Segregation of Duties (SoD) – på svenska ansvarsfördelning – är en grundläggande säkerhetsprincip inom Identity and Access Management (IAM). Principen innebär att ingen enskild person ska ha tillgång till att ensam genomföra en hel kritisk process. Syftet är att minimera risken för bedrägerier, misstag och maktmissbruk.

SoD är ett krav i flera regelverk som GreenTyre Recycling AB som "viktig entitet" under NIS2-direktivet måste förhålla sig till:

- NIS2-direktivet (EU 2022/2555), Art. 21 – krav på intern kontroll och åtkomstkontroll
- ISO/IEC 27002:2022, kontroll 5.3 – Segregation of duties
- ISO/IEC 27002:2022, kontroll 5.15 – Access control
- GDPR (EU 2016/679) – principen om minsta privilegium (Least Privilege)

2. Syfte och mål

Syftet med denna labb är att implementera och verifiera Segregation of Duties i en Active Directory-miljö med hjälp av IGDLA-principen. Labben demonstrerar hur behörigheter struktureras så att:

- IT-personal har full åtkomst till konfidentiella resurser och delade resurser
- HR- och ekonomipersonal har läsbehörighet till delade resurser
- HR- och ekonomipersonal saknar helt åtkomst till konfidentiella resurser
- Behörigheter hanteras centralt via grupper – aldrig direkt på användarnivå

3. IGDLA-principen

IGDLA är en hierarkisk modell för behörighetshantering i Active Directory. Modellen definierar en tydlig kedja från användare till resursåtkomst och är Microsofts rekommenderade metod för skalbar och säker behörighetsstyrning.

Bokstav	Nivå	Beskrivning
I	Identity (Identitet)	Enskilda användarkonton – t.ex. Anna.IT, Maria.HR
G	Global Group	Grupper som speglar avdelningar/roller – t.ex. GL_IT, GL_HR
D	Domain Local Group	Grupper kopplade till en specifik resurs + behörighet – t.ex. DL_Konfidentiellt_FC
L	Local Group	Används i större miljöer med flera domäner (ej tillämpat i denna labb)
A	Access (Åtkomst)	Den faktiska resursen –

		mappar, system, delade kataloger

Nyckelregeln i IGDLA: Behörigheter tilldelas aldrig direkt till användare (I) eller globala grupper (G). Alla NTFS-rättigheter sätts uteslutande på Domain Local-grupper (DL), som i sin tur innehåller globala grupper, som i sin tur innehåller användare. Detta ger maximal flexibilitet – vid organisationsförändringar räcker det att ändra gruppmedlemskap, aldrig mappbehörigheter.

4. Labbmiljö (Virtualiserad)

Komponent	Detaljer
Domänkontrollant	Windows Server 2019 – mylab.local (192.168.122.194)
Klientdator	Windows 11 – domänansluten till mylab.local
Domän	mylab.local
AD-verktyg	Active Directory Users and Computers (ADUC) Och Administrative Center
Delade mappar	C:\Shares\Konfidentiellt och C:\Shares\Delade
Testanvändare	Anna.IT (IT), Maria.HR (HR), Johan.ACC (Accounting)

5. Konfiguration

5.1 Testanvändare (I – Identity)

Tre testanvändare skapades i respektive avdelnings OU för att spegla GreenTyre Recycling AB:s organisationsstruktur:

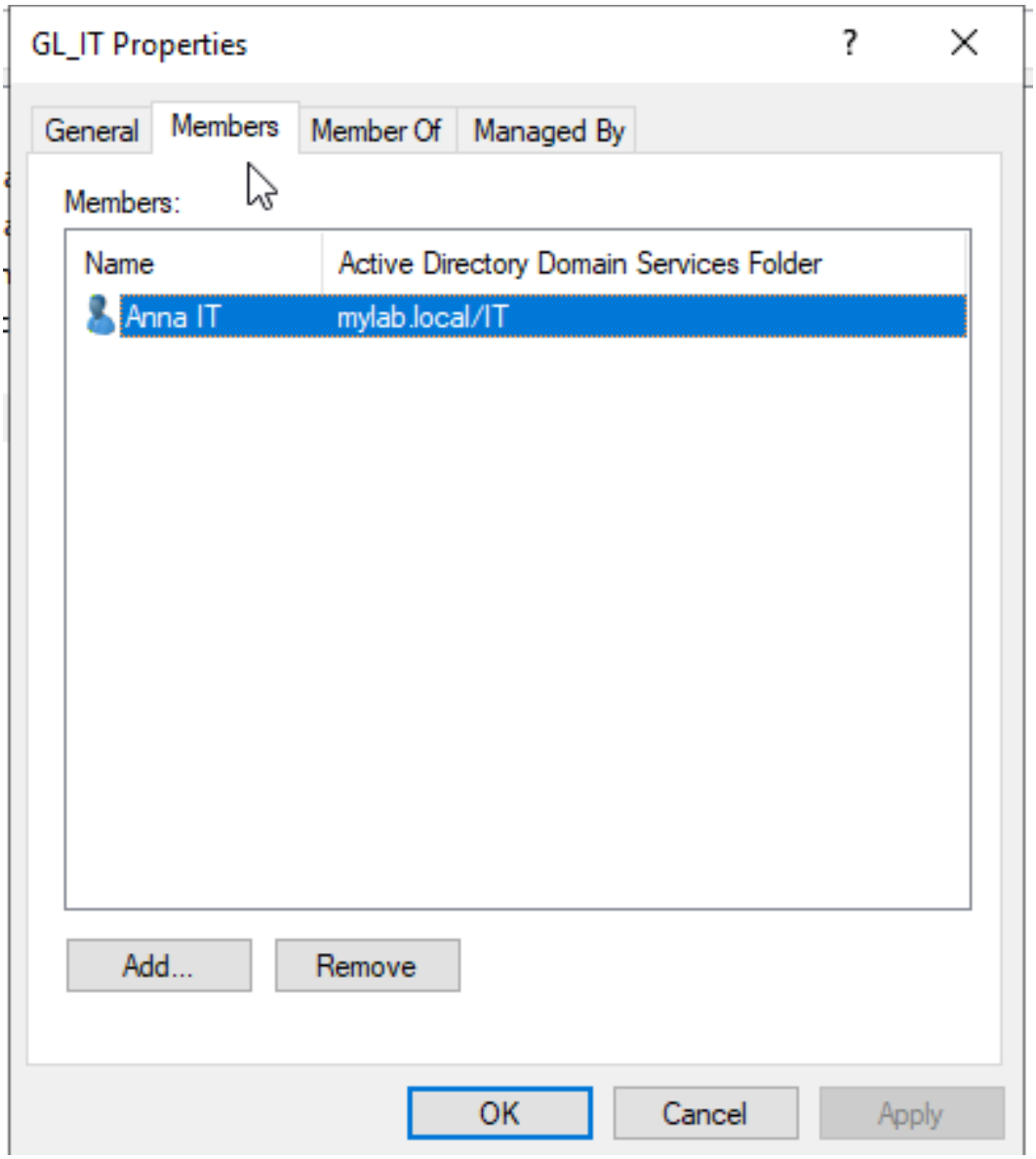
Namn	Konto	Avdelning	OU
Anna IT	Anna.IT	IT	OU=IT,DC=mylab,
Maria HR	Maria.HR	HR	OU=HR,DC=mylab
Johan ACC	Johan.ACC	Accounting	OU=Accounting,DC=mylab

5.2 Globala grupper (G – Global Groups)

Globala säkerhetsgrupper skapades för att representera avdelningar. Dessa grupper speglar organisationsstrukturen och fungerar som bärare av användaridentiteter in i behörighetskedjan:

Grupp	Scope	Innehåller
GL_IT	Global Security	Anna.IT
GL_HR	Global Security	Maria.HR
GL_Accounting	Global Security	Johan.ACC

Screenshot nedan visar GL_IT med Anna IT som medlem i ADUC:



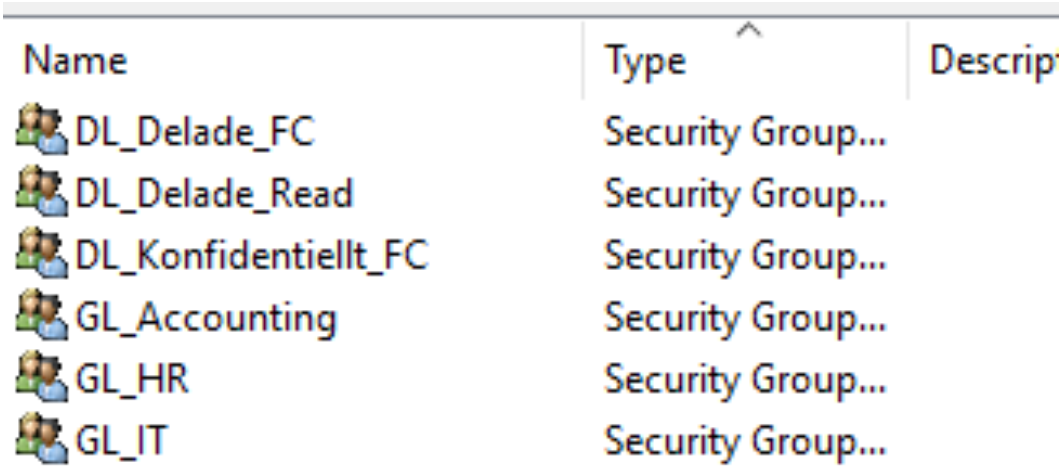
Figur 1 – GL_IT med Anna IT som medlem (ADUC, Members-fliken)

5.3 Domain Local-grupper (DL – Domain Local Groups)

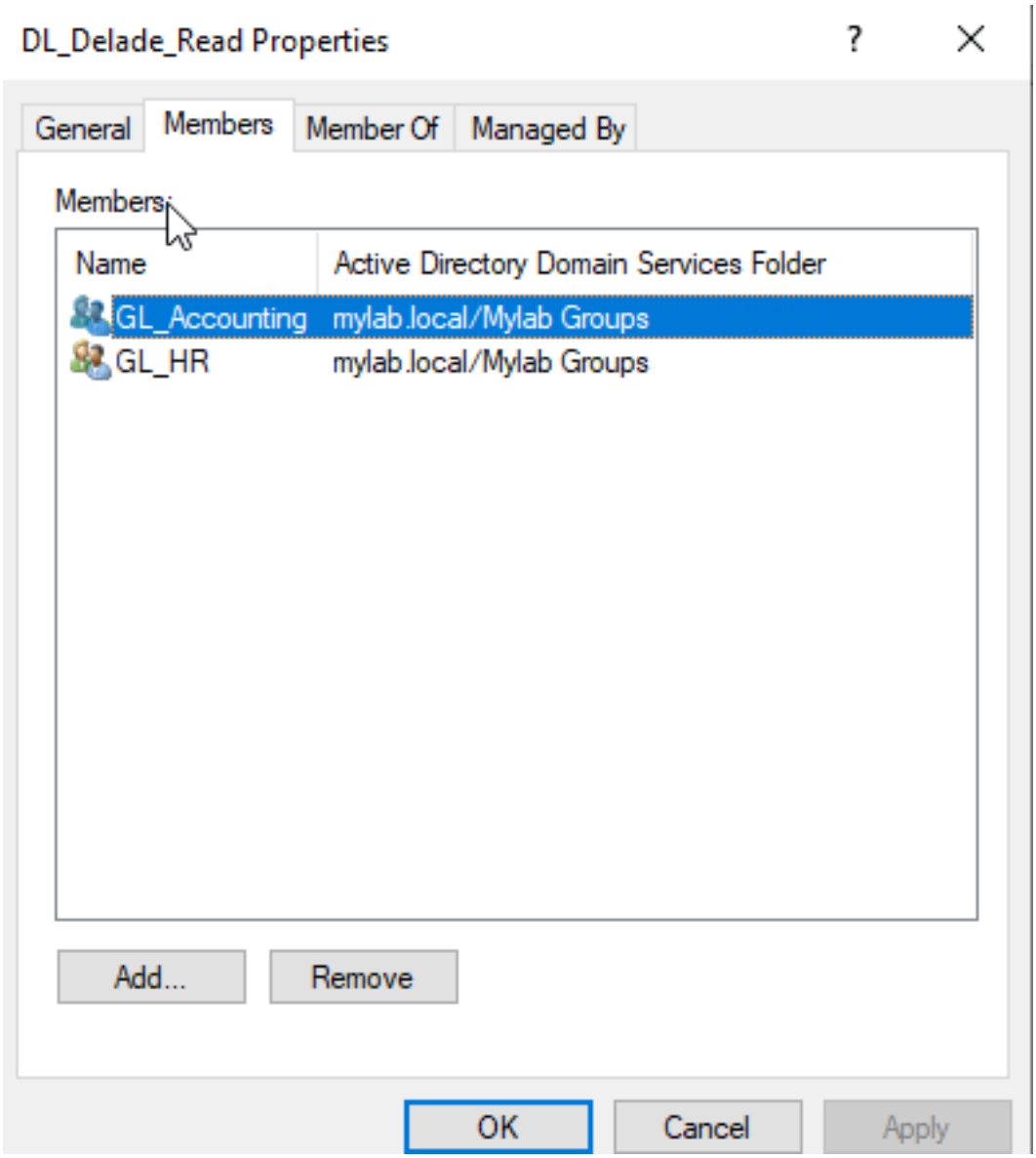
Domain Local-grupper skapades per resurs och behörighet. Dessa grupper tilldelas direkt till mapparna via NTFS-behörigheter och innehåller de globala grupperna – aldrig enskilda användare:

Grupp	Scope	Innehåller (G-grupper)	Resurs
DL_Konfidentiellt_FC	Domain Local	GL_IT	C:\Shares\Konfidentiellt
DL_Delade_FC	Domain Local	GL_IT	C:\Shares\Delade
DL_Delade_Read	Domain Local	GL_HR, GL_Accounting	C:\Shares\Delade

Screenshot nedan visar alla skapade grupper i OU=Mylab Groups samt DL_Delade_Read med GL_HR och GL_Accounting som medlemmar:



Figur 2 – Alla GL och DL-grupper i OU=Mylab Groups (ADUC)

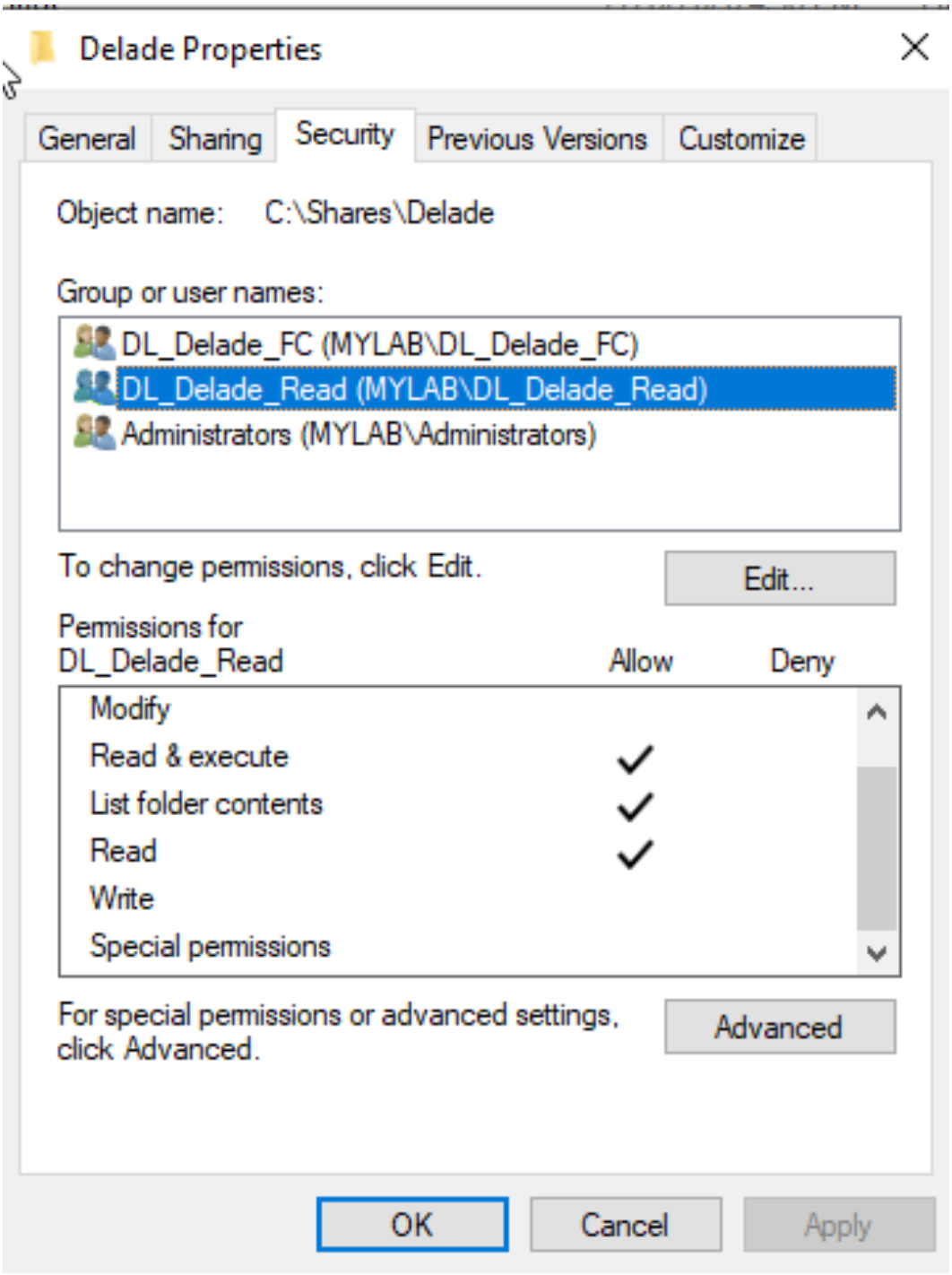


Figur 3 – DL_Delade_Read med GL_Accounting och GL_HR som medlemmar

5.4 Mappbehörigheter (A – Access)

Två delade mappar skapades under C:\Shares\. Arvsrättigheter inaktiverades (inheritance disabled) på båda mapparna och behörigheter sattes explicit via Domain Local-grupperna:

Mapp	Grupp (DL)	NTFS-behörighet
C:\Shares\Konfidentiellt	DL_Konfidentiellt_FC	Full Control
C:\Shares\Konfidentiellt	BUILTIN\Administrators	Full Control
C:\Shares\Delade	DL_Delade_FC	Full Control
C:\Shares\Delade	DL_Delade_Read	Read & Execute



Figur 4 – Säkerhetsfliken för C:\Shares\Delade med DL_Delade_FC och DL_Delade_Read

6. IGDLA-kedjan visualiserad

Nedan illustreras den fullständiga behörighetskedjan för varje användare enligt IGDLA-modellen:

Anna.IT (IT-avdelningen)
Anna.IT → GL_IT → DL_Konfidentiellt_FC → C:\Shares\Konfidentiellt (Full Control)
Anna.IT → GL_IT → DL_Delade_FC → C:\Shares\Delade (Full Control)
IT-personal har full kontroll på båda resurserna. Motivering: IT-avdelningen ansvarar för systemen och behöver kunna administrera samtliga kataloger.

Maria.HR (HR-avdelningen)
Maria.HR → GL_HR → DL_Delade_Read → C:\Shares\Delade (Read & Execute)
Maria.HR → GL_HR → [ingen DL] → C:\Shares\Konfidentiellt (NEKAD)
HR-personal kan läsa delade dokument men saknar helt åtkomst till konfidentiella resurser. Detta implementerar SoD – HR kan inte ta del av konfidentiell IT-information.

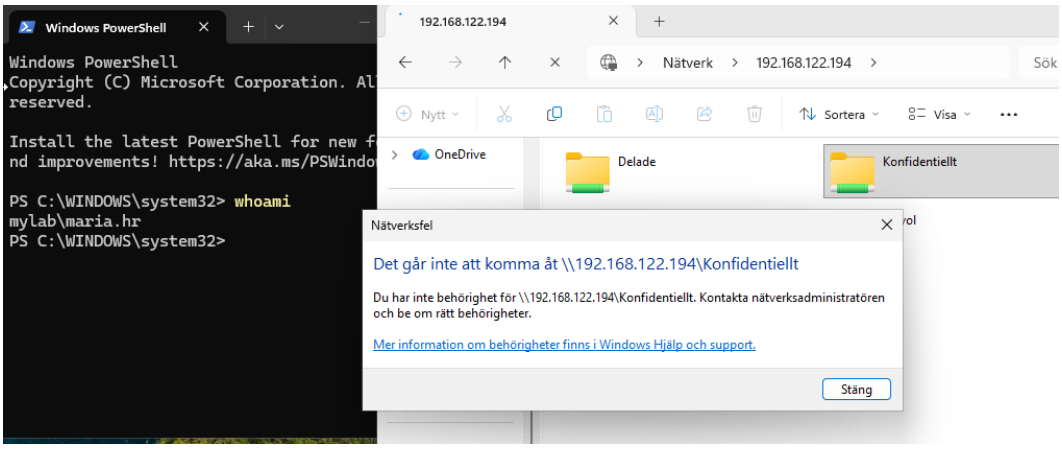
Johan.ACC (Ekonomiavdelningen)
Johan.ACC → GL_Accounting → DL_Delade_Read → C:\Shares\Delade (Read & Execute)
Johan.ACC → GL_Accounting → [ingen grupp] → C:\Shares\Konfidentiellt (NEKAD)
Ekonomipersonal har samma behörighetsprofil som HR – läsåtkomst till delade resurser, ingen åtkomst till konfidentiella resurser.

7. Verifiering och testresultat

Åtkomstkontrollen verifierades på en domänansluten Windows 11-klient genom att logga in som respektive testanvändare och försöka nå de delade resurserna via UNC-sökvägar (\\192.168.122.194\Konfidentiellt och \\192.168.122.194\Delade).

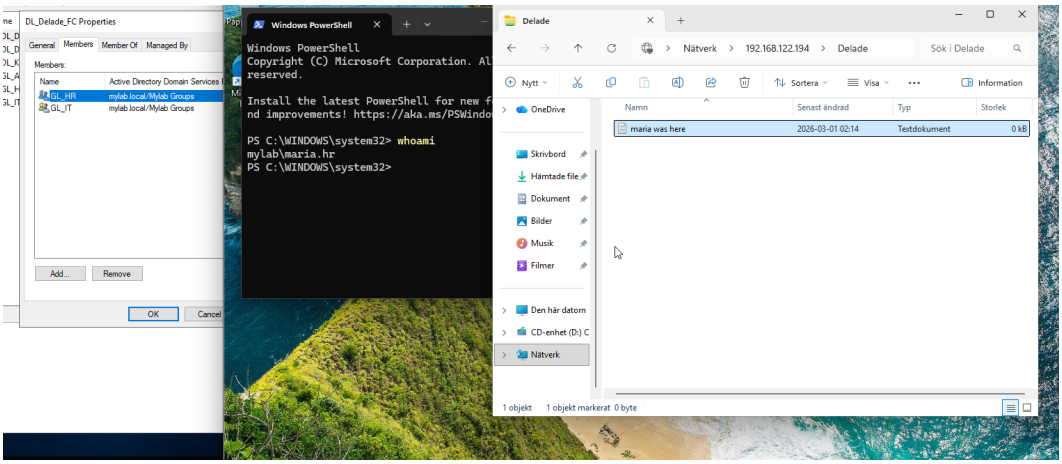
Användare	Resurs	Förväntat	Resultat
Anna.IT	\\srv\Konfidentiellt	Full Control	**OK – Åtkomst beviljad**
Anna.IT	\\srv\Delade	Full Control	**OK – Åtkomst beviljad**
Maria.HR	\\srv\Konfidentiellt	NEKAD	**OK – Åtkomst nekad**
Maria.HR	\\srv\Delade	Read Only	**OK – Läsåtkomst**

Bevis 1: Maria.HR nekas åtkomst till \\192.168.122.194\Konfidentiellt. PowerShell-kommandot "whoami" bekräftar att inloggningen sker som mylab\maria.hr:



Figur 5 – Maria.HR (mylab\maria.hr) nekas åtkomst till \\Konfidentiellt (Windows 11-klient)

Bevis 2: Maria.HR har läsåtkomst till \\192.168.122.194\Delade. Mappen kan öppnas men inga filer kan skapas eller raderas:



Figur 6 – Maria.HR kan öppna Delade (läsåtkomst bekräftad)

8. Koppling till NIS2 och ISO 27001

Krav/Kontroll	Källa	Hur labben uppfyller kravet
Art. 21.2(a) – Åtkomstkontroll	NIS2	IGDLA-principen säkerställer att behörigheter hanteras systematiskt och centralt
Art. 21.2(b) – Minsta privilegium	NIS2	HR och Accounting har enbart de rättigheter de behöver för sitt arbete
Kontroll 5.3 – Segregation of duties	ISO 27002:2022	IT-personal och övriga avdelningar har separerade behörighetsprofiler

Kontroll 5.15 – Access control	ISO 27002:2022	Åtkomst styrs via gruppbaserade NTFS-rättigheter med arvsrättigheter inaktiverade

9. Slutsats och reflektion

Labben demonstrerar hur IGDLA-principen effektivt implementerar Segregation of Duties i en Active Directory-miljö. Genom att strukturera behörigheter i en tydlig kedja – användare till globala grupper till domain local-grupper till resurser – uppnås:

- Skalbarhet: Nya användare behöver bara läggas i rätt Global Group, inget annat ändras
- Säkerhet: Ingen direkt koppling mellan användare och resurser – alltid via grupper
- Revision: Behörighetsstrukturen är lättgranskad och dokumenterbar
- NIS2-efterlevnad: Tydlig ansvarsfördelning som uppfyller Art. 21 krav på åtkomstkontroll
- Least Privilege: Varje avdelning har exakt de rättigheter som behövs – inget mer