



# **SAS® Security Model Design Golden Rules, Validation, and Monitoring**

Starting at 11am

# Host

## Caroline Scottow



# Presenters

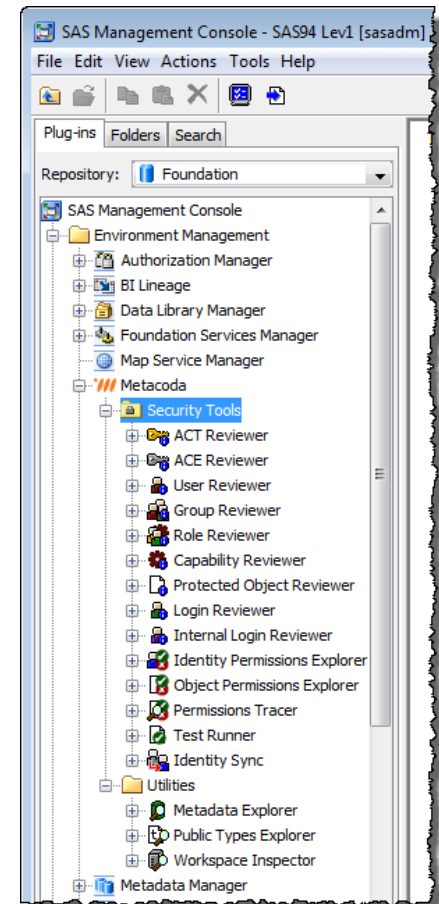
David Stern, SAS

Paul Homes, Metacoda



# About Metacoda

-  ... since 2007
- Provide add-ons to SAS® Software for enhanced **metadata** visibility and exploitation
  - Metacoda Identity Sync
  - Metacoda Security Plug-ins
  - Metacoda Testing Framework
  - Metacoda Utility Plug-ins - free
  - Custom Tasks (for SAS Enterprise Guide & AMO) - free
- Goals:
  - Improve your productivity through enhanced metadata visibility
  - Helping to keep your SAS platform secure



# Managing the webinar

- In Listen Mode
- Control bar opened with the white arrow in the orange box





[bit.ly/SASUKMetacodaWebinar](https://bit.ly/SASUKMetacodaWebinar)




# Designing a Security Model

# Designing a Security Model is Harder than it Looks

- SAS authorization is flexible, robust and performant
- Does not impose strong standards
- Allows complex, confusing or bad design
- Common problems:
  - Authorization conflicts result in users having too much or too little access
  - Hard for administrators to see why a permission is granted or denied
  - Security admin is time-consuming and frustrating
  - Disorientation when staff transition between projects
  - Hard to promote content between SAS deployments while maintaining correct permissions
  - Hard to support multi-tenancy





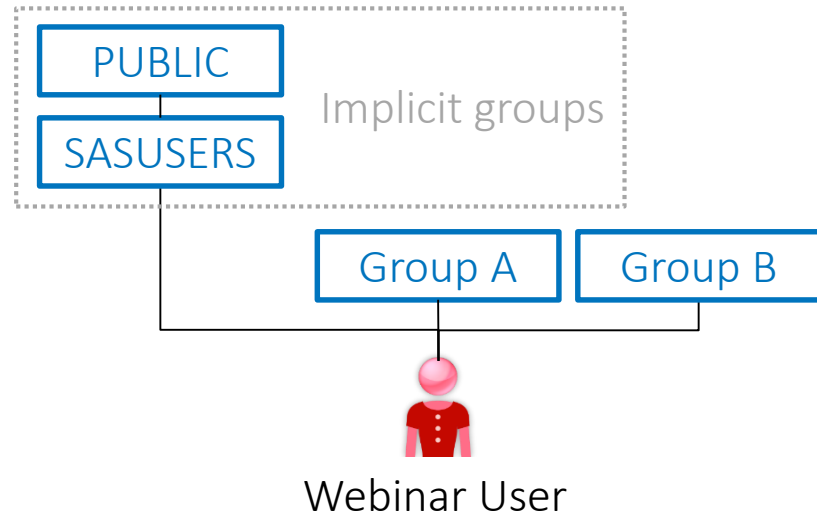
# Quiz

## Authorization Conflicts

## Quiz

### About the questions

- Each questions is about a user called **Webinar User**
- Webinar User is a direct member of Group A and Group B
- Webinar User is also a member of SASUSERS and PUBLIC



- Each question simply asks whether Webinar User has ReadMetadata access to a folder: **yes** or **no**

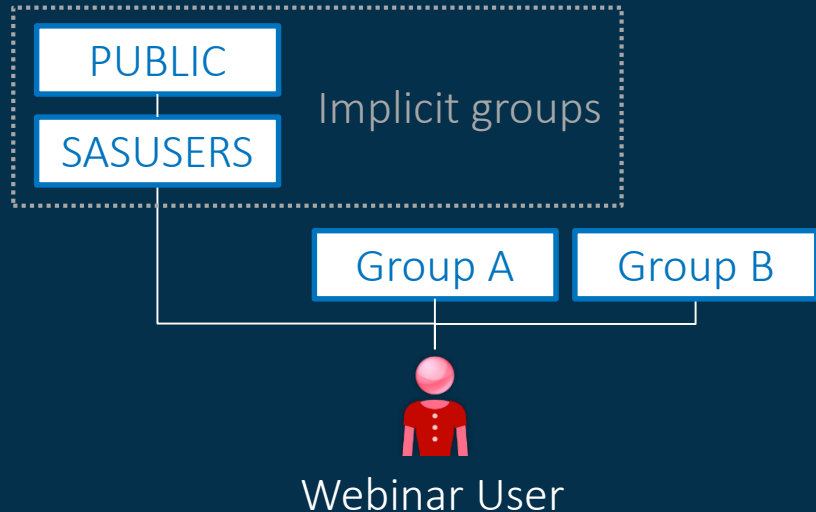
# Question 1

## Can Webinar User see Folder 1?

- An entry in the Default ACT grants RM to Webinar User
- Folder 1 has a direct ACE, denying RM to PUBLIC
- Webinar User is implicitly a member of the group PUBLIC
- Notice this question has one ACT and one ACE
- Can Webinar User see Folder 1?

Definitions:

- ACT: Access Control Template
- ACE: Access Control Entry
- RM: Read Metadata



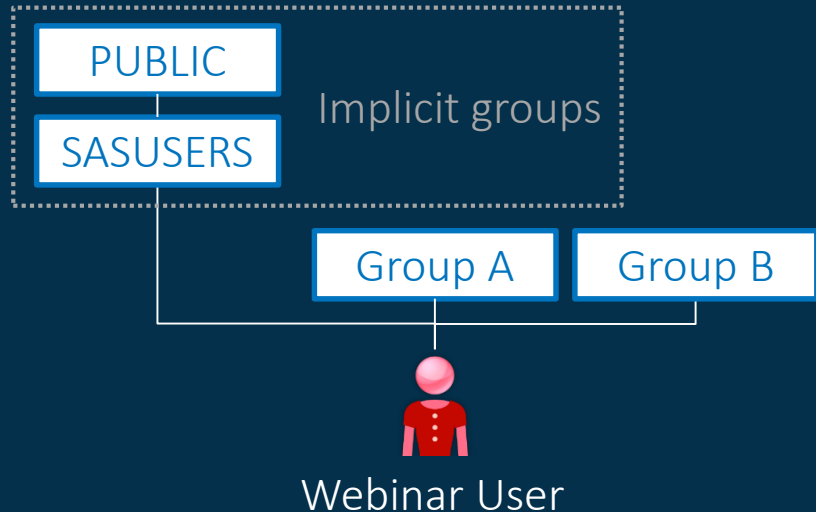
# Question 2

## Can Webinar User see Folder 2?

- An ACT which denies RM to PUBLIC is applied to Folder 2
  - An ACT which grants RM to Group A is applied to Folder 2
  - Webinar User is a member of Group A directly
  - Webinar User is implicitly a member of the group PUBLIC
- 
- Can Webinar User see Folder 2?

Definitions:

- ACT: Access Control Template
- ACE: Access Control Entry
- RM: Read Metadata



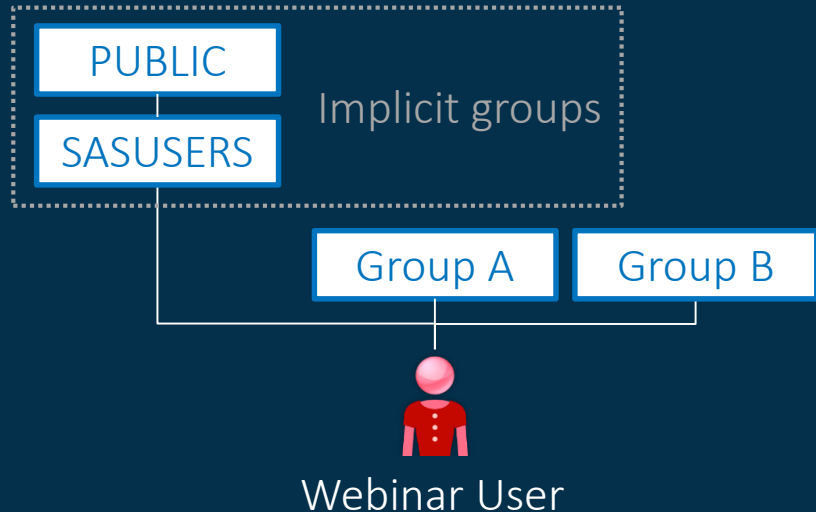
# Question 3

## Can Webinar User see Folder 3?

- An ACT which denies RM to Group A is applied to Folder 3
- An ACE which grants RM to Group B is applied to Folder 3
- Webinar User is a member of both Group A and Group B directly
- Notice this question has one ACT and one ACE
- Can Webinar User see Folder 3?

Definitions:

- ACT: Access Control Template
- ACE: Access Control Entry
- RM: Read Metadata



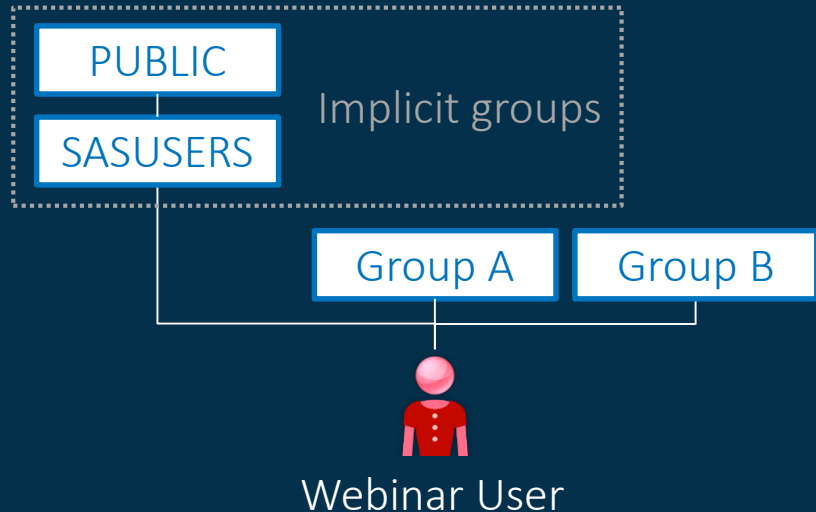
# Question 4

## Can Webinar User see Folder 4?





- An ACT which denies RM to Group A is applied to Folder 4
- An ACT which grants RM to Group B is applied to Folder 4
- Webinar User is a direct member of both Group A and Group B
- Can Webinar User see Folder 4?

Definitions:

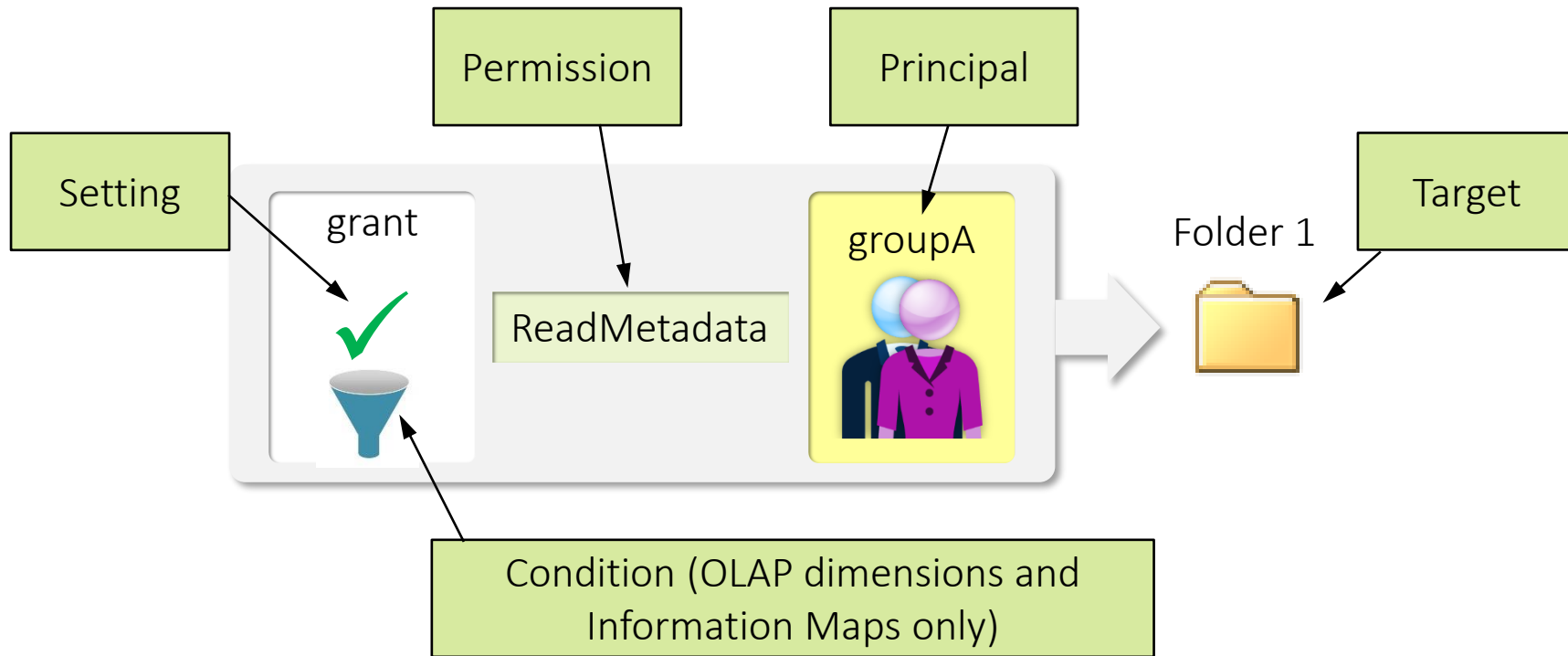
- ACT: Access Control Template
- ACE: Access Control Entry
- RM: Read Metadata



# Answers

- Question 1
  - Can Webinar User see Folder 1? No 
- Question 2
  - Can Webinar User see Folder 2? Yes 
- Question 3
  - Can Webinar User see Folder 3? Yes 
- Question 4
  - Can Webinar User see Folder 4? No 

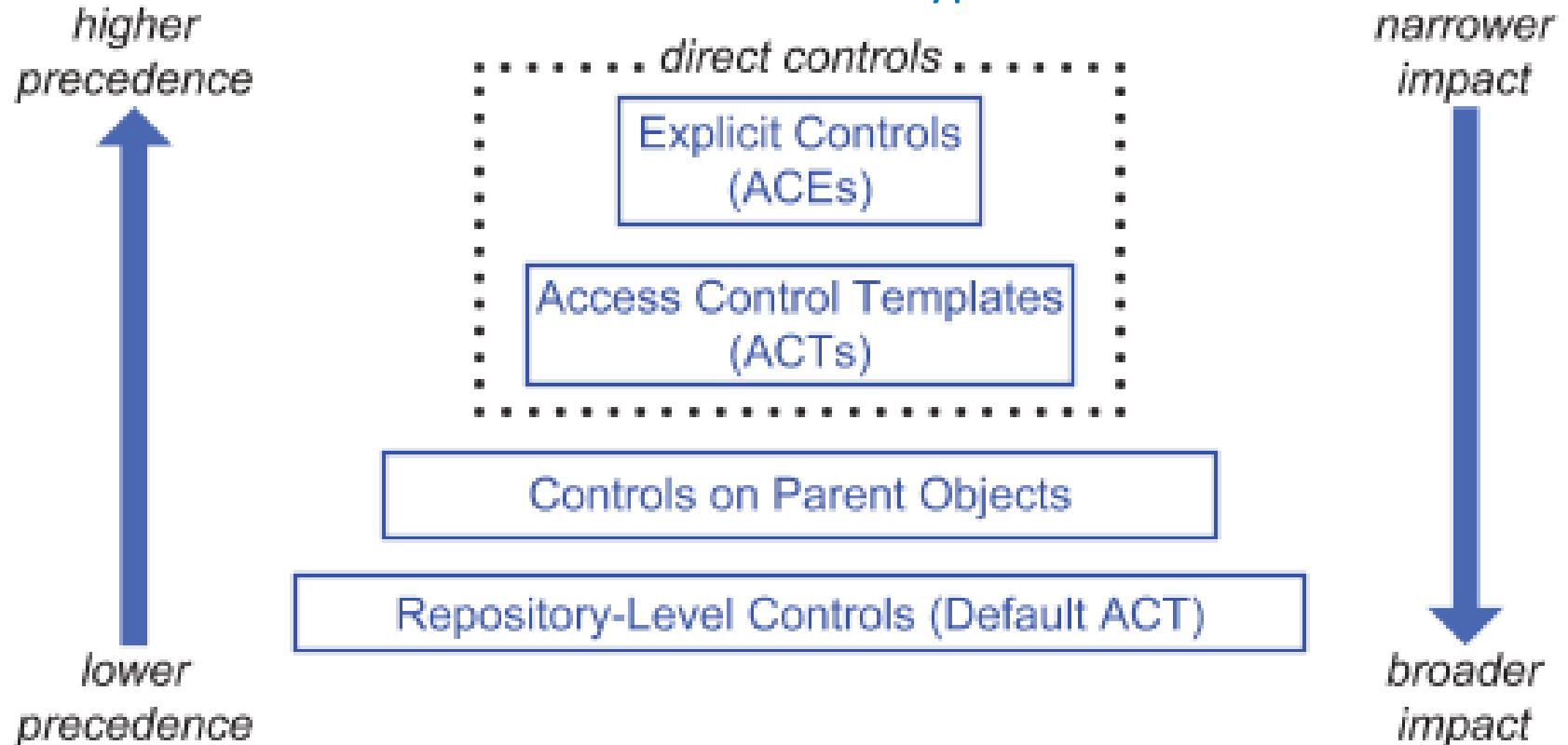
# Access Controls





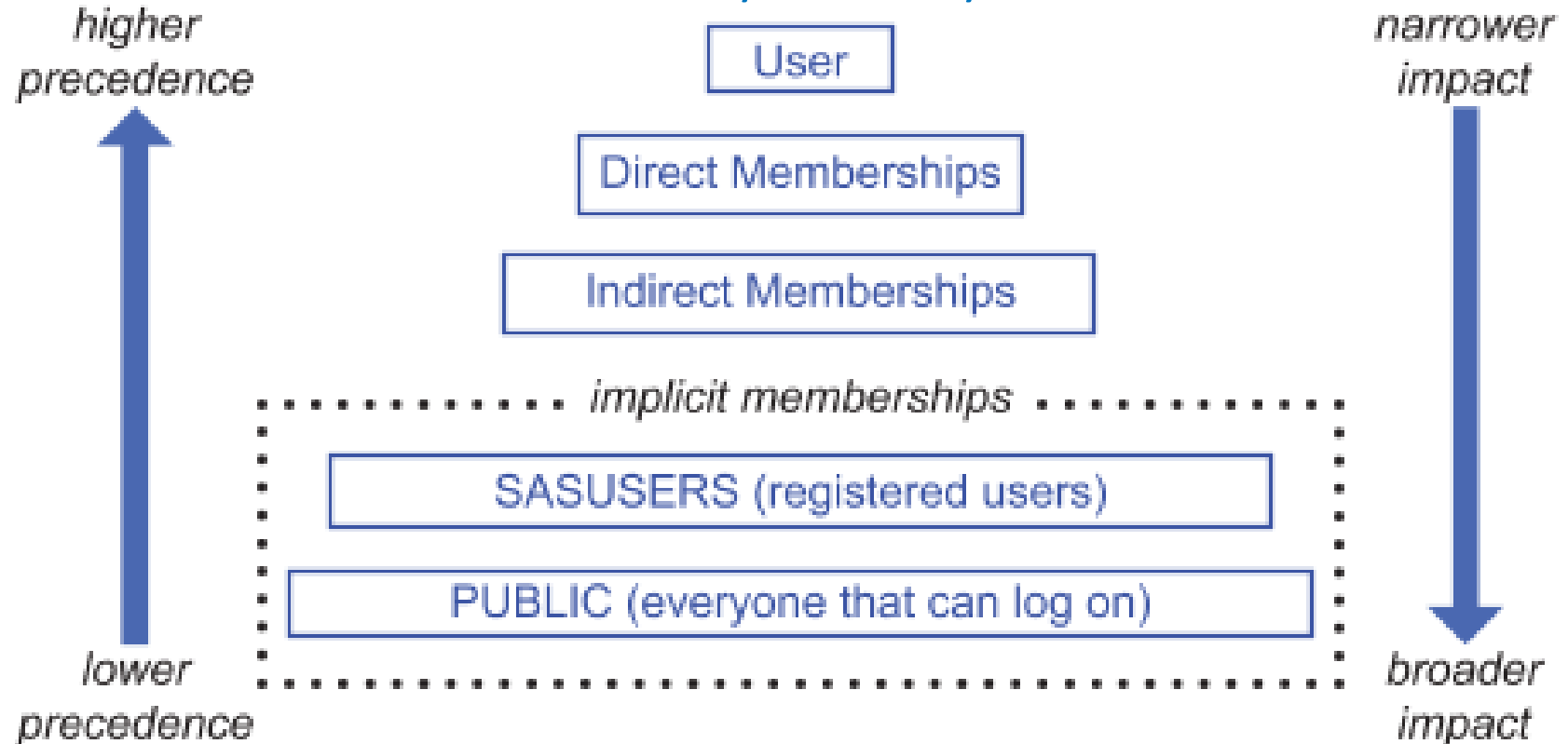
# Resolving SAS 9 Metadata permission conflicts

## Access Control Type

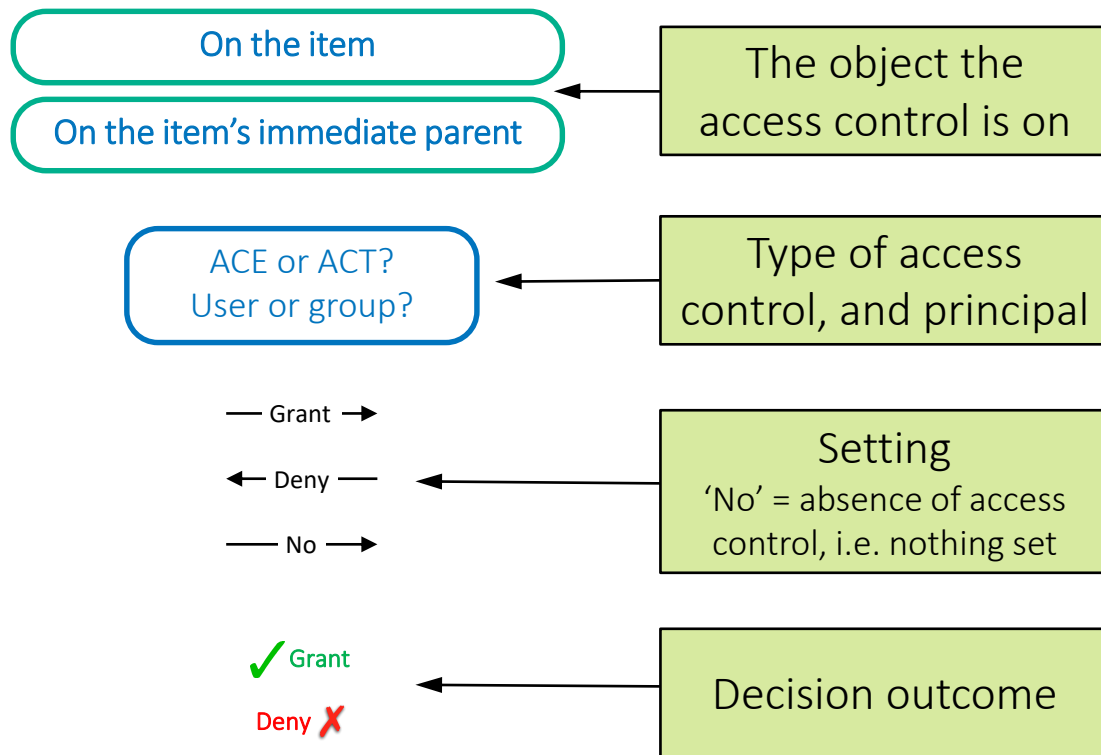


# Resolving SAS 9 Metadata permission conflicts

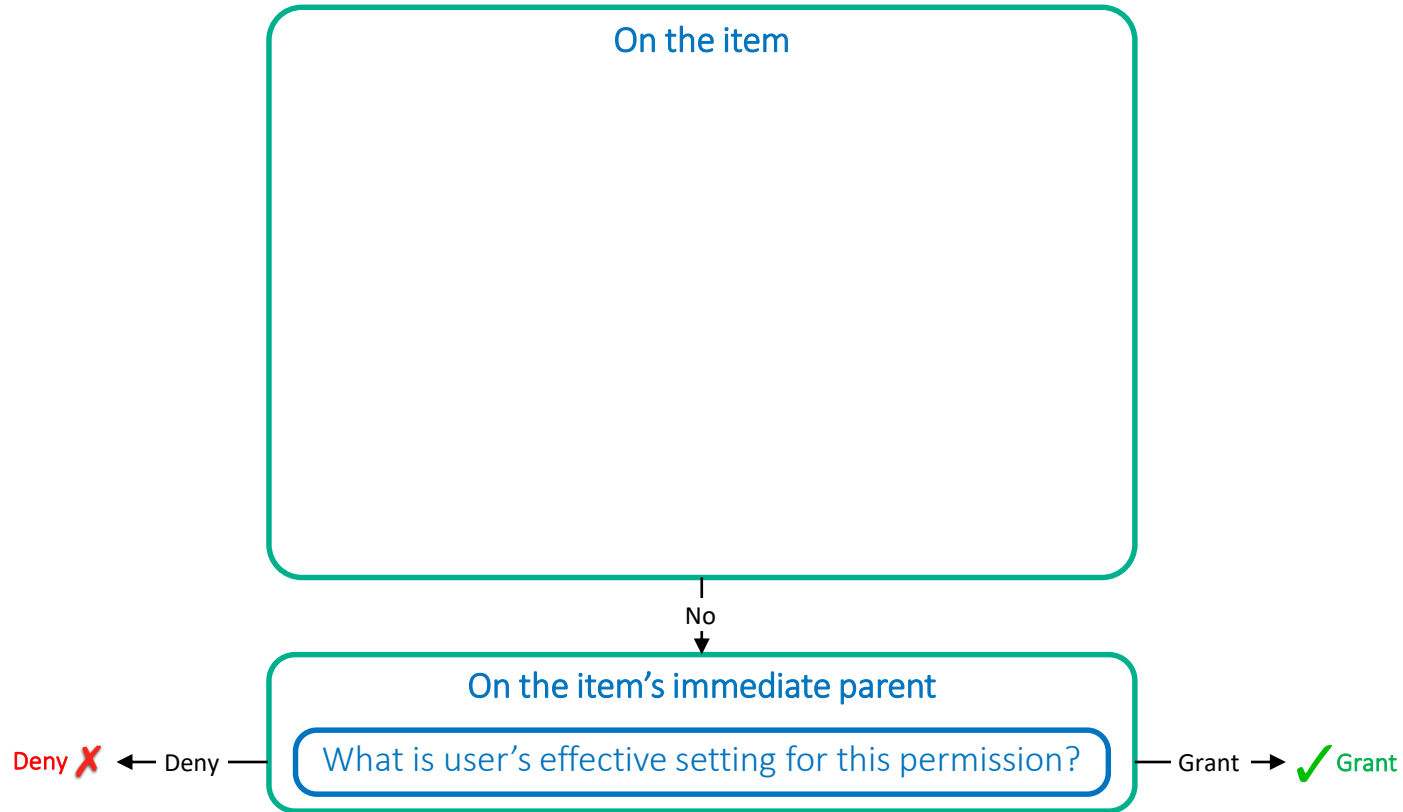
## Identity Hierarchy



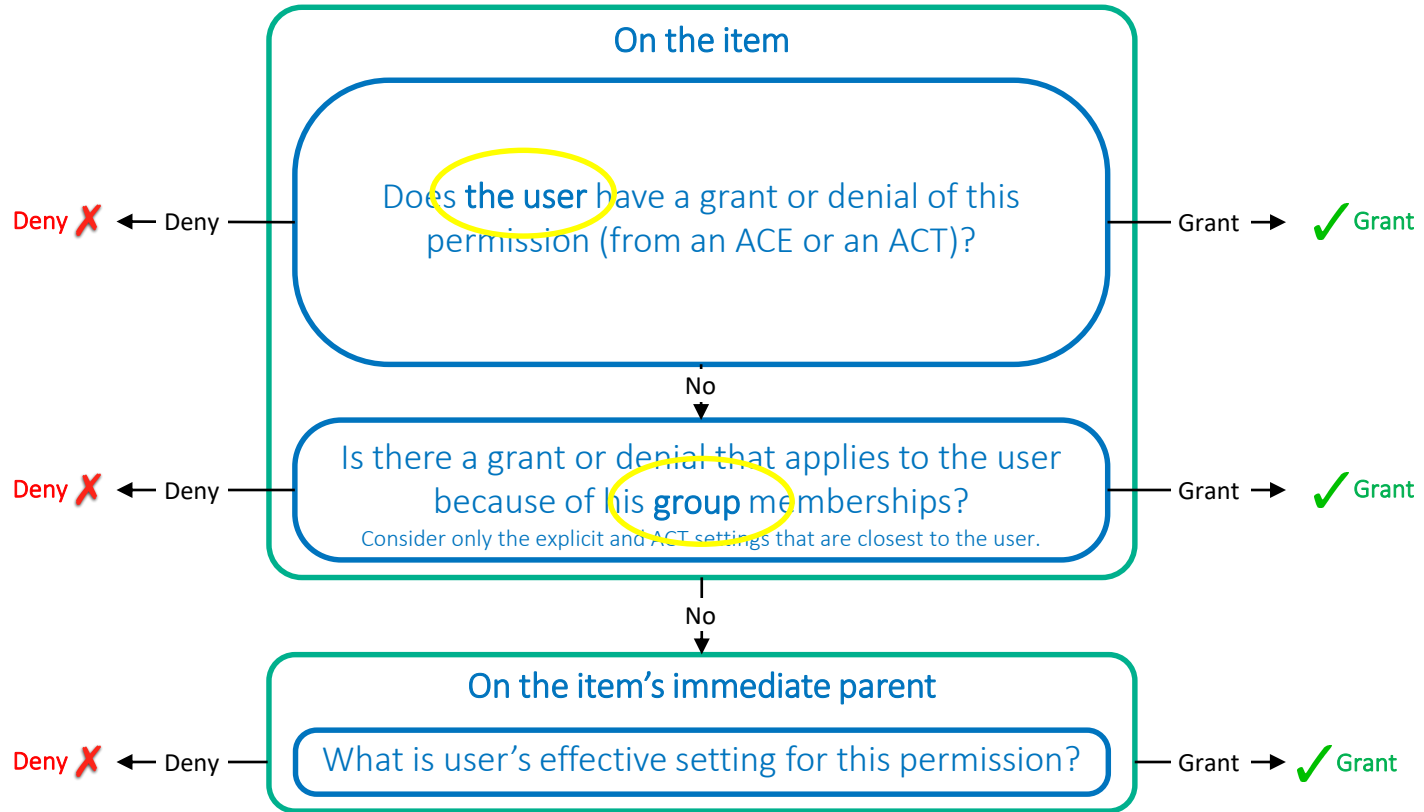
# Authorization Decision flowchart legend



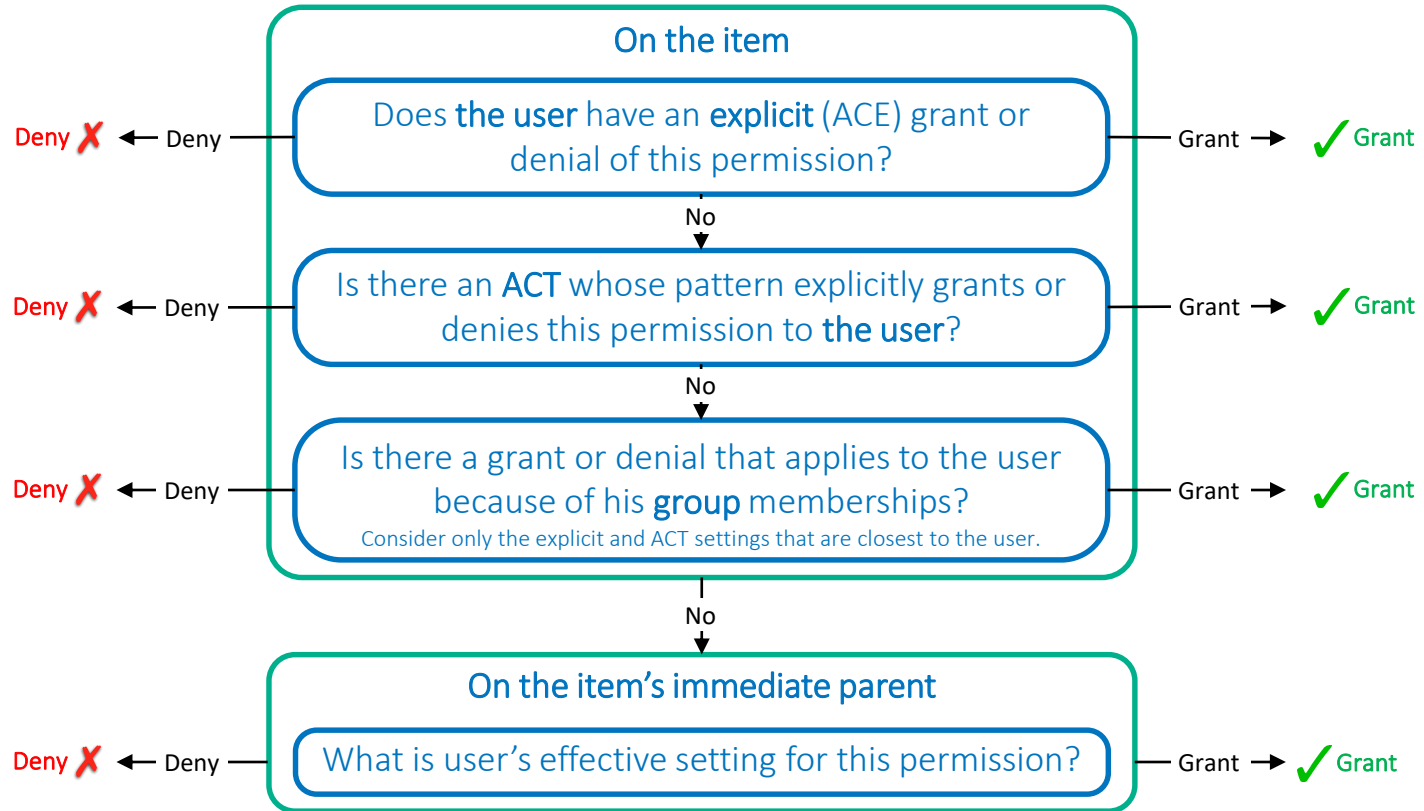
# 1. Settings on an item have priority over settings on the item's parents



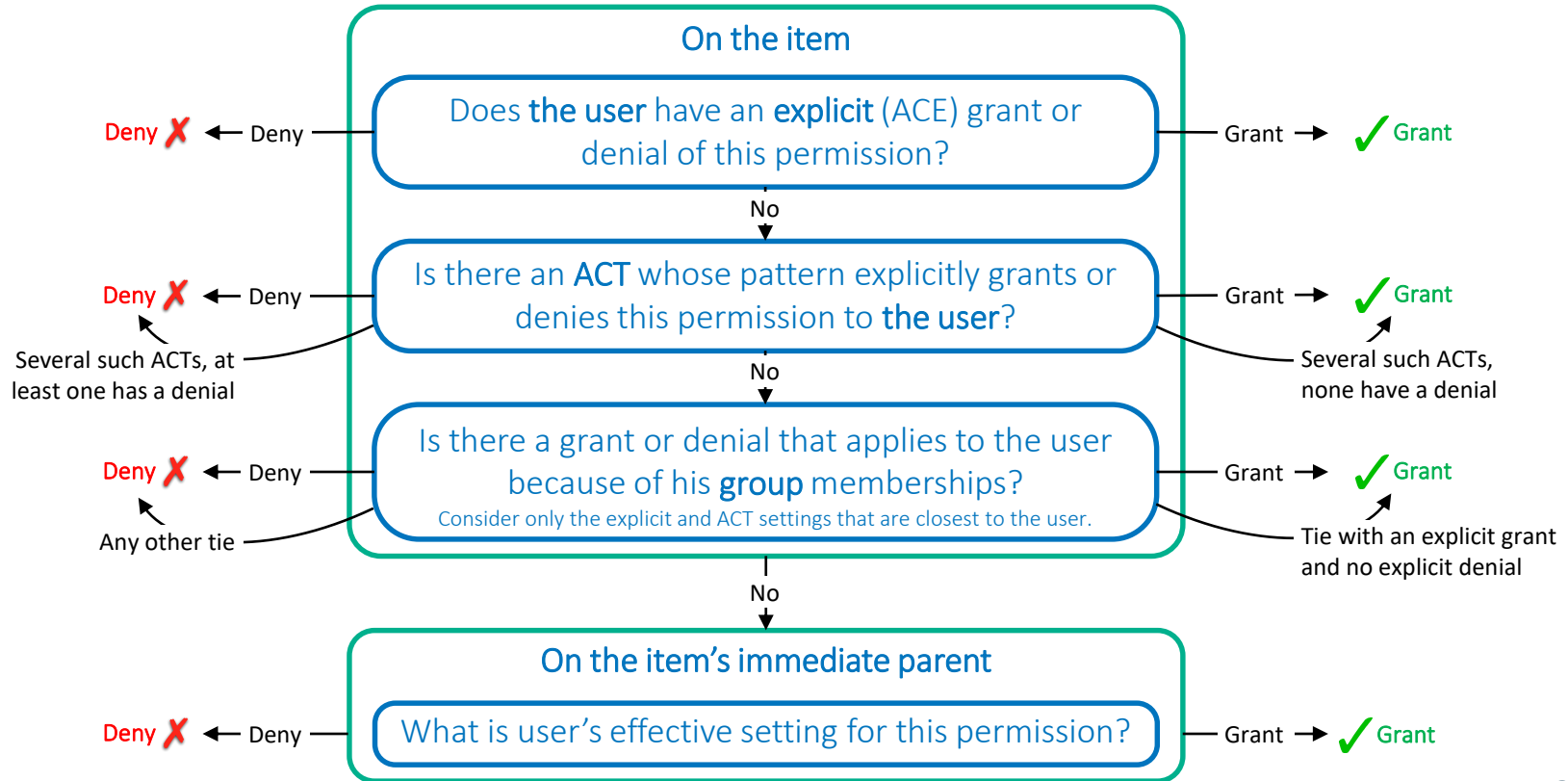
## 2. Conflicting settings on an item are resolved by identity precedence



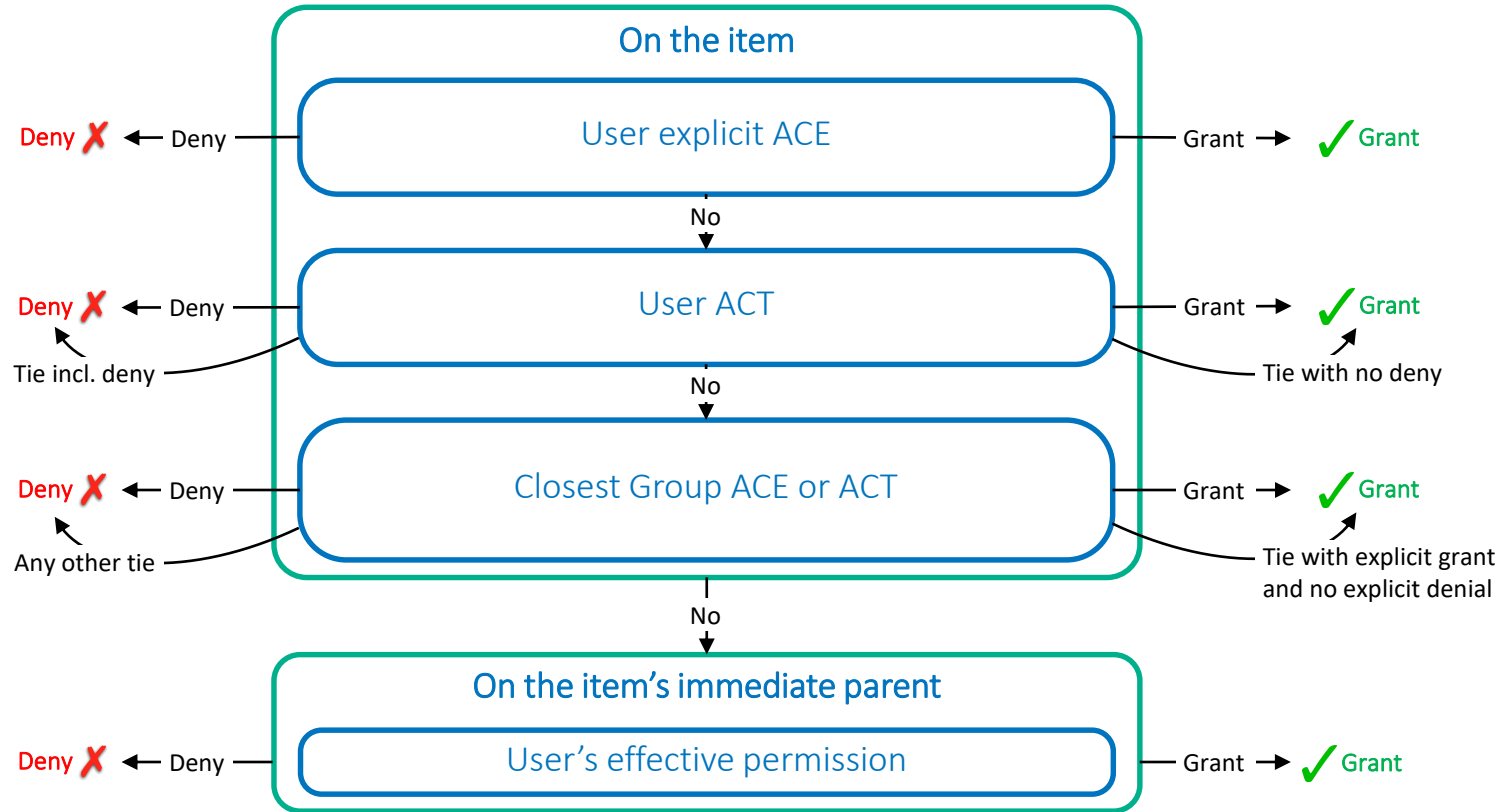
### 3. In an identity precedence tie, explicit settings have priority over ACT settings



## 4. In an identity precedence tie that isn't resolved by the preceding rule, the outcome is a denial

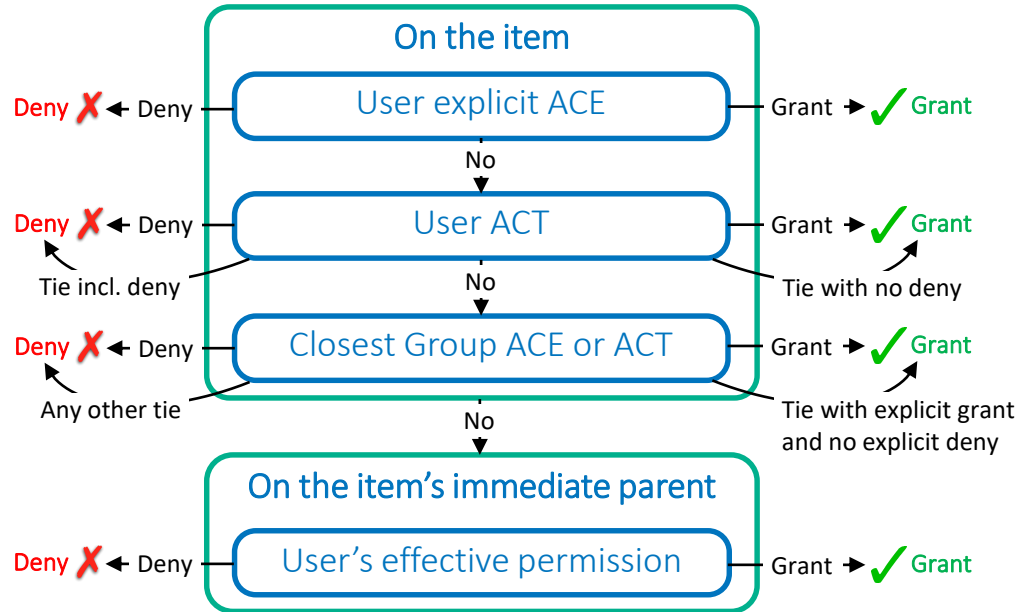


# Simplify the words





# Small simplified version



# Question 1

Can Webinar User see Folder 1?



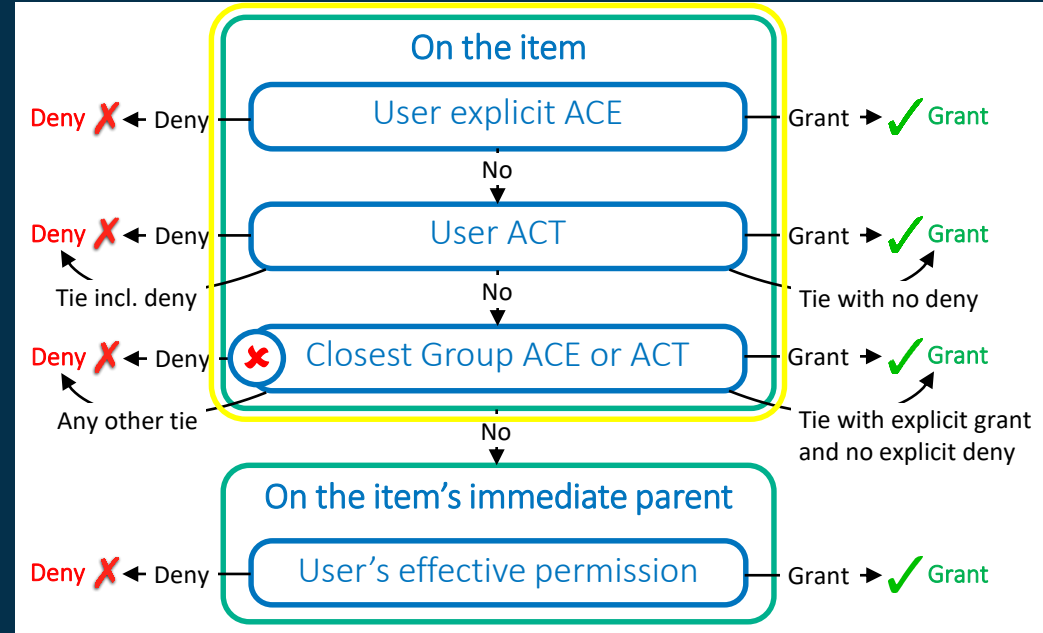
Winning Grant



Winning Deny

- An entry in the Default ACT grants RM to Webinar User
- Folder 1 has a direct ACE, denying RM to PUBLIC
  - Webinar User is implicitly a member of the group PUBLIC
  - Notice this question has one ACT and one ACE
- Can Webinar User see Folder 1?

No 



# Question 2

Can Webinar User see Folder 2?



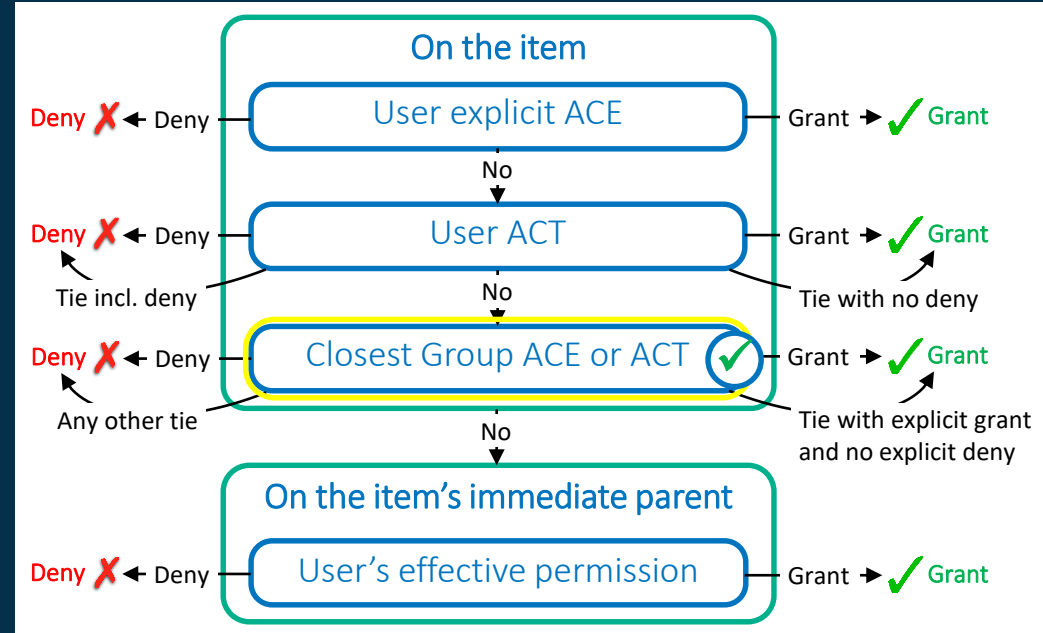
Winning Grant



Winning Deny

- An ACT which denies RM to PUBLIC is applied to Folder 2
- An ACT which grants RM to Group A is applied to Folder 2
- Webinar User is a member of Group A directly
- Webinar User is implicitly a member of the group PUBLIC
- Can Webinar User see Folder 2?

Yes



# Question 3

Can Webinar User see Folder 3?



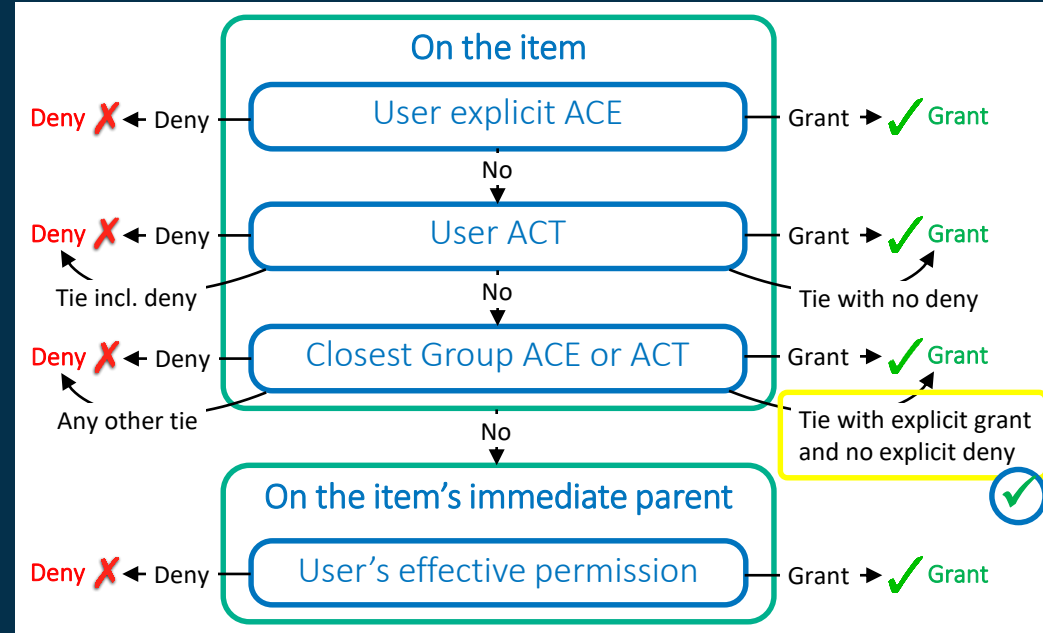
Winning Grant



Winning Deny

- An ACT which denies RM to Group A is applied to Folder 3
- An ACE which grants RM to Group B is applied to Folder 3
- Webinar User is a member of both Group A and Group B directly
- Notice this question has one ACT and one ACE
- Can Webinar User see Folder 3?

Yes



# Question 4

Can Webinar User see Folder 4?



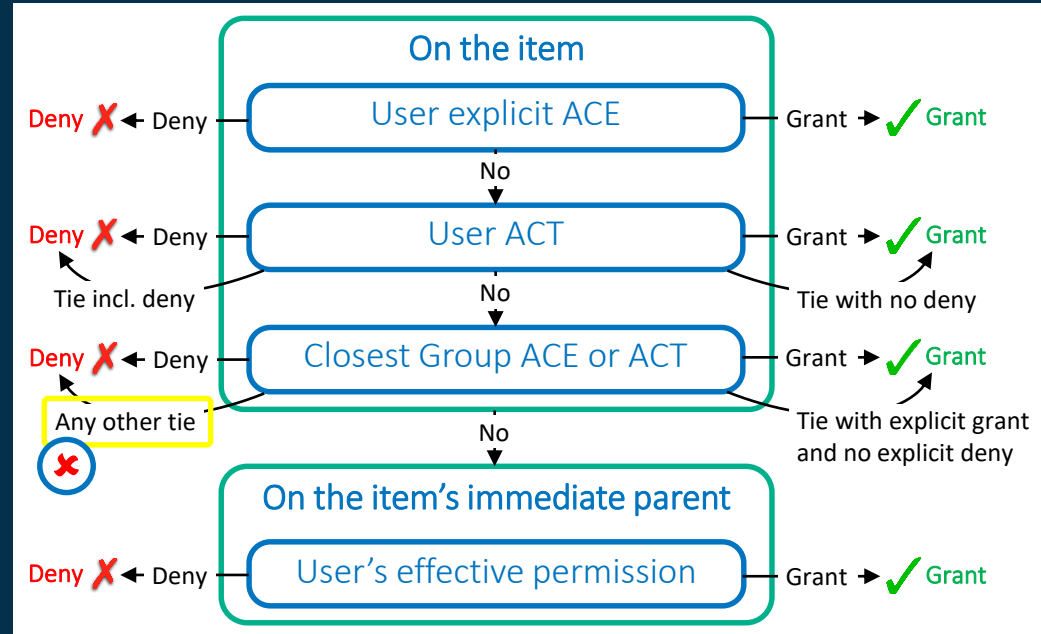
Winning Grant



Winning Deny

- An ACT which denies RM to Group A is applied to Folder 4
- An ACT which grants RM to Group B is applied to Folder 4
  - Webinar User is a direct member of both Group A and Group B
- Can Webinar User see Folder 4?

No 



# 8 Golden Rules of Security Model Design

- Rule 1: Only use ACTs, never ACEs
- Rule 2: Only add groups to ACTs
- Rule 3: ACTs only *grant* access to explicit groups, never deny
- Rule 4: Where necessary, apply ACTs to deny access to PUBLIC/SASUSERS, in combination with ACTs to grant a reduced set of permissions to explicit groups
- Rule 5: Always Apply the SAS Administrators ACT when PUBLIC and SASUSERS are denied access
- Rule 6: Design your security model first and implement it early
- Rule 7: Apply ACTs to folders where possible
- Rule 8: Name security model objects clearly and simply

# Resources for Administrators

- Golden Rules for Security Model Design

- <https://communities.sas.com/t5/SAS-Communities-Library/Golden-Rules-for-Security-Model-Design/ta-p/373542>
- <https://communities.sas.com/t5/SAS-Communities-Library/Golden-Rules-for-Security-Model-Design-part-2/ta-p/373543>
- <https://communities.sas.com/t5/SAS-Communities-Library/Golden-Rules-for-Security-Model-Design-part-3/ta-p/373547>
- <https://communities.sas.com/t5/SAS-Communities-Library/Golden-Rules-for-Security-Model-Design-part-4/ta-p/373551>
- <https://communities.sas.com/t5/SAS-Communities-Library/Golden-Rules-for-Security-Model-Design-part-5/ta-p/373555>

- Five papers on Recommended SAS 9.4 Security Model Design

- <https://communities.sas.com/t5/SAS-Communities-Library/Five-papers-on-Recommended-SAS-9-4-Security-Model-Design-part-1/ta-p/361569>
- <https://communities.sas.com/t5/SAS-Communities-Library/Five-papers-on-Recommended-SAS-9-4-Security-Model-Design-part-2/ta-p/361575>

- Checklist of SAS Platform Administration Tasks

- <https://communities.sas.com/t5/SAS-Communities-Library/Checklist-of-SAS-Platform-Administration-Tasks/ta-p/223991>

# Validate and report on your security model

- Treat security model design and implementation in a similar way to other project deliverables in your SAS environment:
  - Adopt principles and standards for security model design
  - Design before you build
  - Implementing security is easy (and cheap), design is hard (thus more expensive)
  - Implement according to those standards, and correct deviations from standards
- Test that your security model adheres to your design
- Test that your security model adheres to your adopted standards
  - Manually by visual inspection
  - Write code (export data describing security, compare it to pre-defined rules, compare between environments or compare before and after)
  - Use a third party tool – [Metacoda Security Plug-ins](#) are the best known





# Metacoda

## Demonstration



# Questions?



[bit.ly/SASUKMetacodaWebinar](https://bit.ly/SASUKMetacodaWebinar)

Thank you

[sas.com](https://sas.com)