Assessment/Collection Gap Analysis

Charles Schmidt - Moderator

June 12, 2009

MITRE

Session Agenda

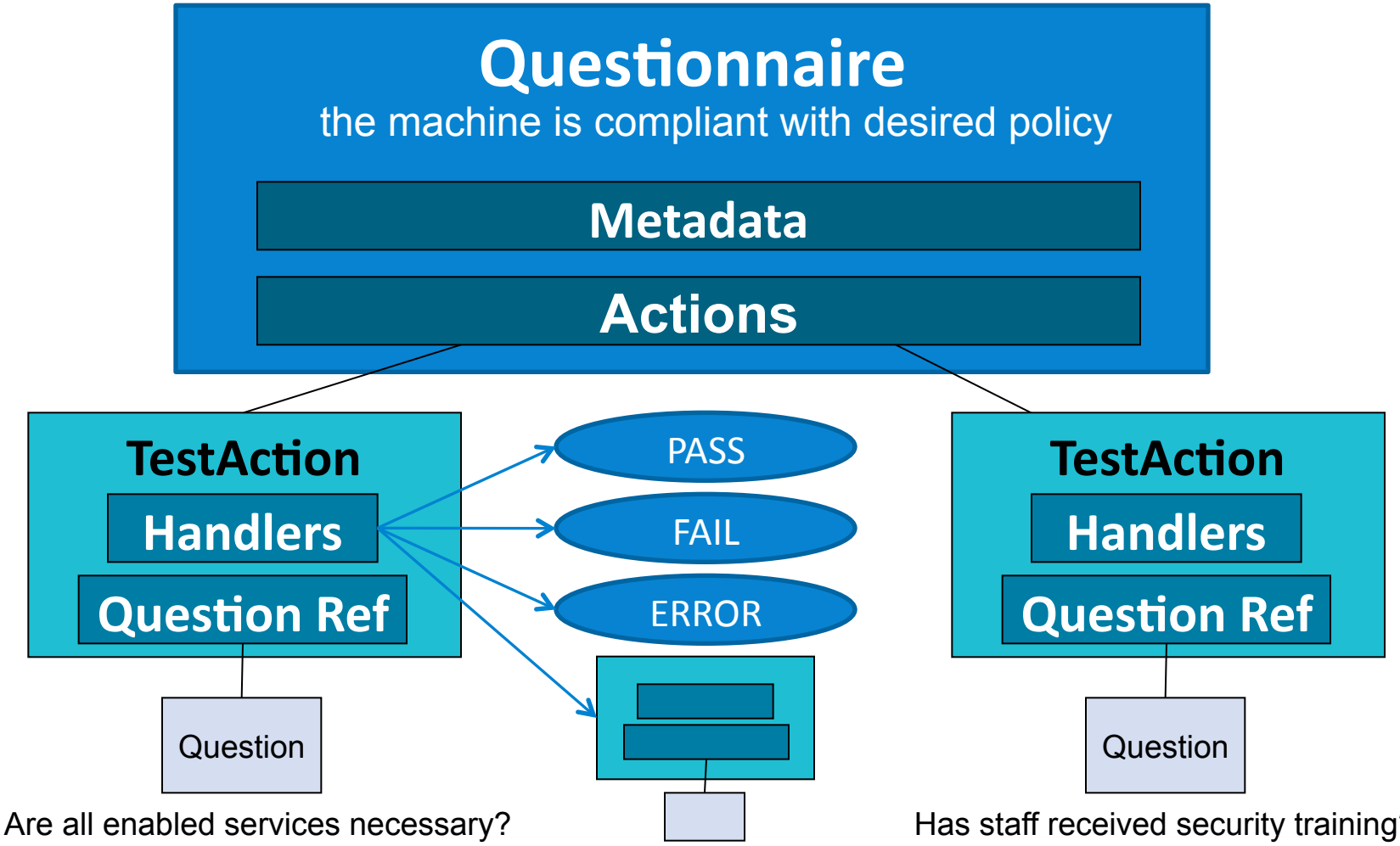
- Introduction to OCIL
  - OCIL – Open Checklist Interactive Language
  - Discussion of use cases and their support
- Introduction to OCRL
  - OCRL – Open Checklist Reporting Language
  - Discussion of use cases and their support
- Other gaps

OCIL – Open Checklist Interactive Language

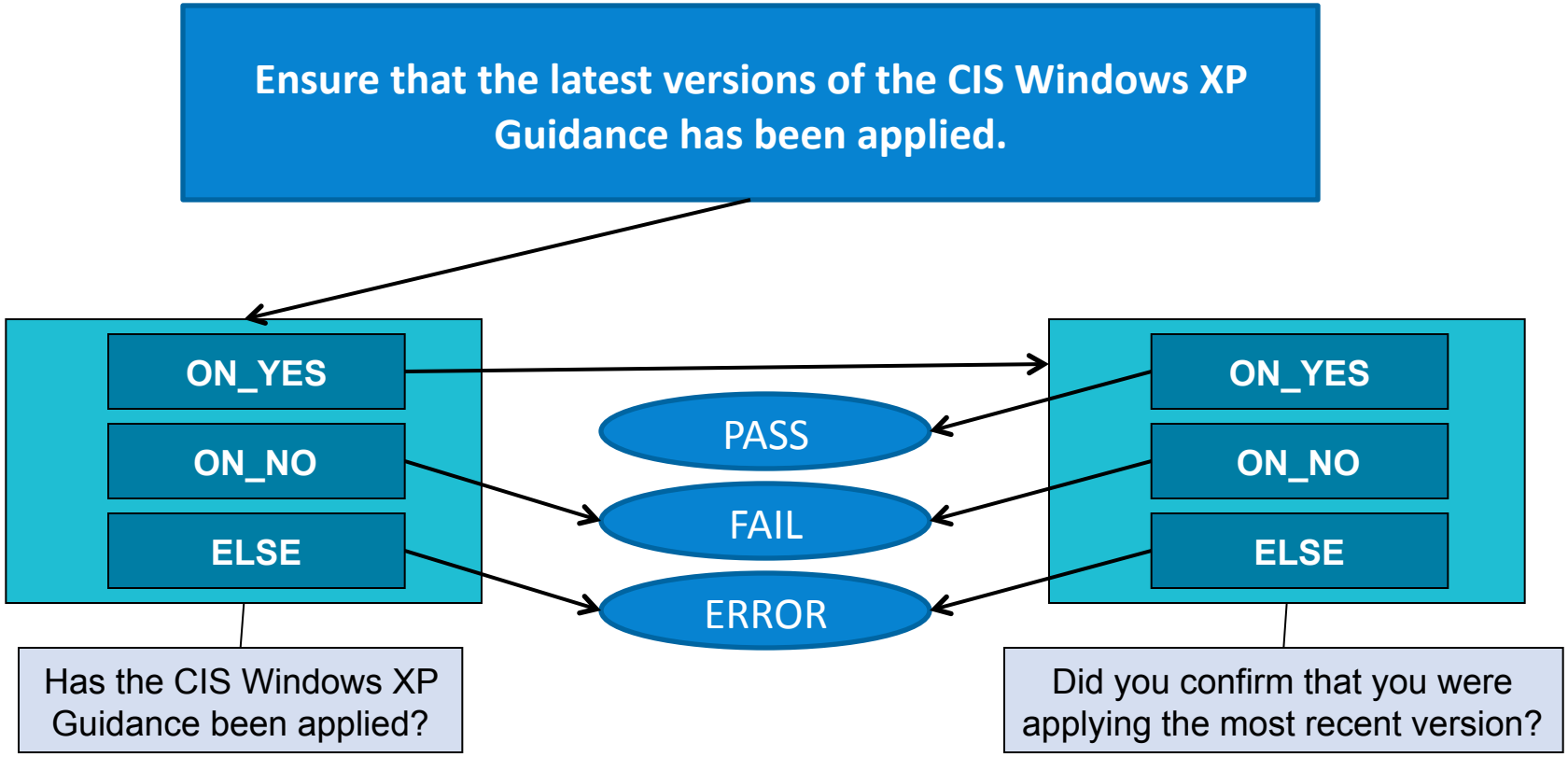
- Support of user question-answer interaction in checklists
- User responses can be Boolean, free text, numeric, or selected from a list of choices
- Language also supports exceptional responses (unknown, not tested, not applicable, error)
- Questions may be presented with a list of steps
  - User follows steps to determine their answer to the question
- Follow-on structures support sophisticated questionnaires
  - Responses combined using AND/OR operations
  - Forking of follow-on questions based on user responses
- Includes reporting structures to record relevant information

http://scap.nist.gov/specifications/ocil/

Structure of an OCIL Questionnaire



OCIL Questionnaire Example



OCIL Use Case

- Some recommendations cannot be automatically tested
  - Information is not stored on a system
    - "Is the server room door locked?"
  - The user is being assessed
    - "Do you lock your safe at the end of every day?"
  - The question is too abstract for automatic checking
    - "Are all unnecessary services disabled?"
- OCIL allows checklists to receive and evaluate information when that information cannot be collected and/or evaluated autonomously
  - Supports simple responses
    - Evaluation of responses limited to exact match, ranges (numeric), and pattern matching (free text)
  - Returns results compatible with XCCDF scoring
  - Broken into discrete entities ("questionnaires") that can be referenced from XCCDF Rules

OCIL Use Case Discussion

- Is there community need for this use case?
- Does OCIL meet this use case?
- Are there other use cases or variants appropriate to OCIL?

Expansions to OCIL

- Artifacts
  - The artifact is not evaluated, but is stored with results.
  - Intended to support auditors who require some artifact to back up user assertions
    - Current: Do you have a fire safety policy? [yes/no]
    - Proposed: … and identify the file that describes the policy.
    - Policy file would not be “evaluated” but link would appear in results
- Variables
  - Import from XCCDF
  - In questions?
    - Change what is asked
  - In handlers?
    - Change the conditions under which certain actions are taken (chained TestActions) or which results are returned

Expansions to OCIL - continued

- Unevaluated collection
  - Not evaluated, but used to collect info
  - Akin to using OVAL Objects without OVAL Tests/States
- OCIL "Profiles"
  - Internal tuning of variable settings
  - Change the handler structures
    - E.g. affect the chain of follow-on questions
  - Use cases
    - Support stand-alone OCIL
    - Profile selection controlled by variables (and XCCDF exports)?
  - Issues
    - Is this moving "policy decisions" into OCIL?

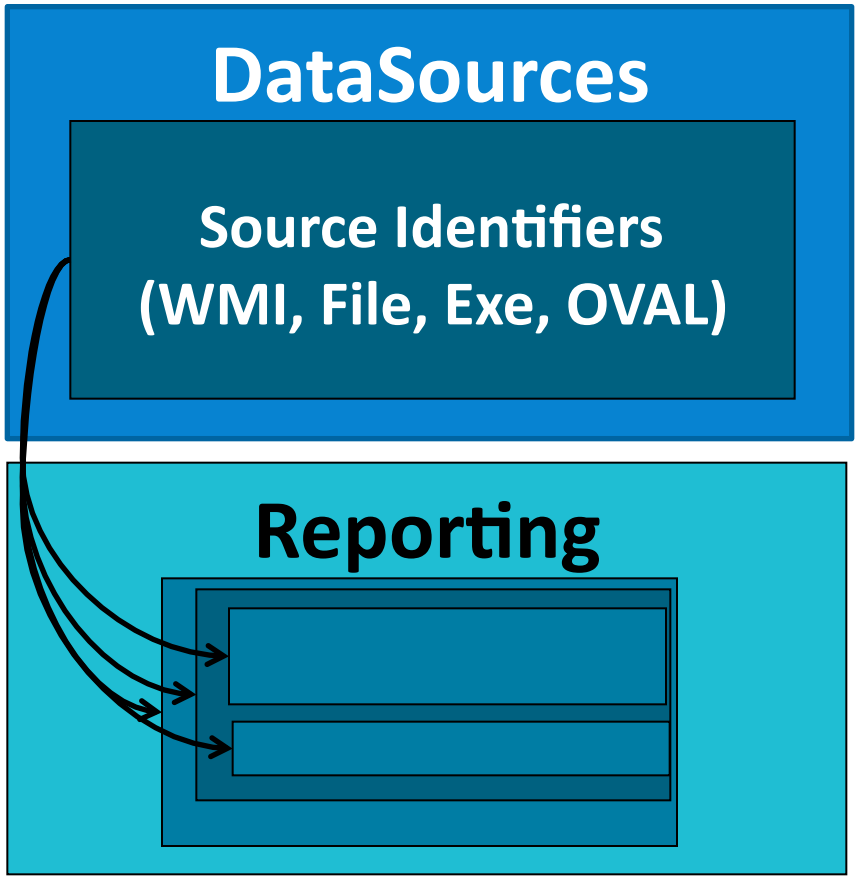
OCRL – Open Checklist Reporting Language

- Supports collection of system state information and formatting it into a report
  - OCRL does no evaluating of state – just collection and reporting
  - Report is a tool that allows a reader to evaluate a compliance question
  - A subsequent activity (e.g. OCIL questionnaire) would be needed to get a result to a checklist tool

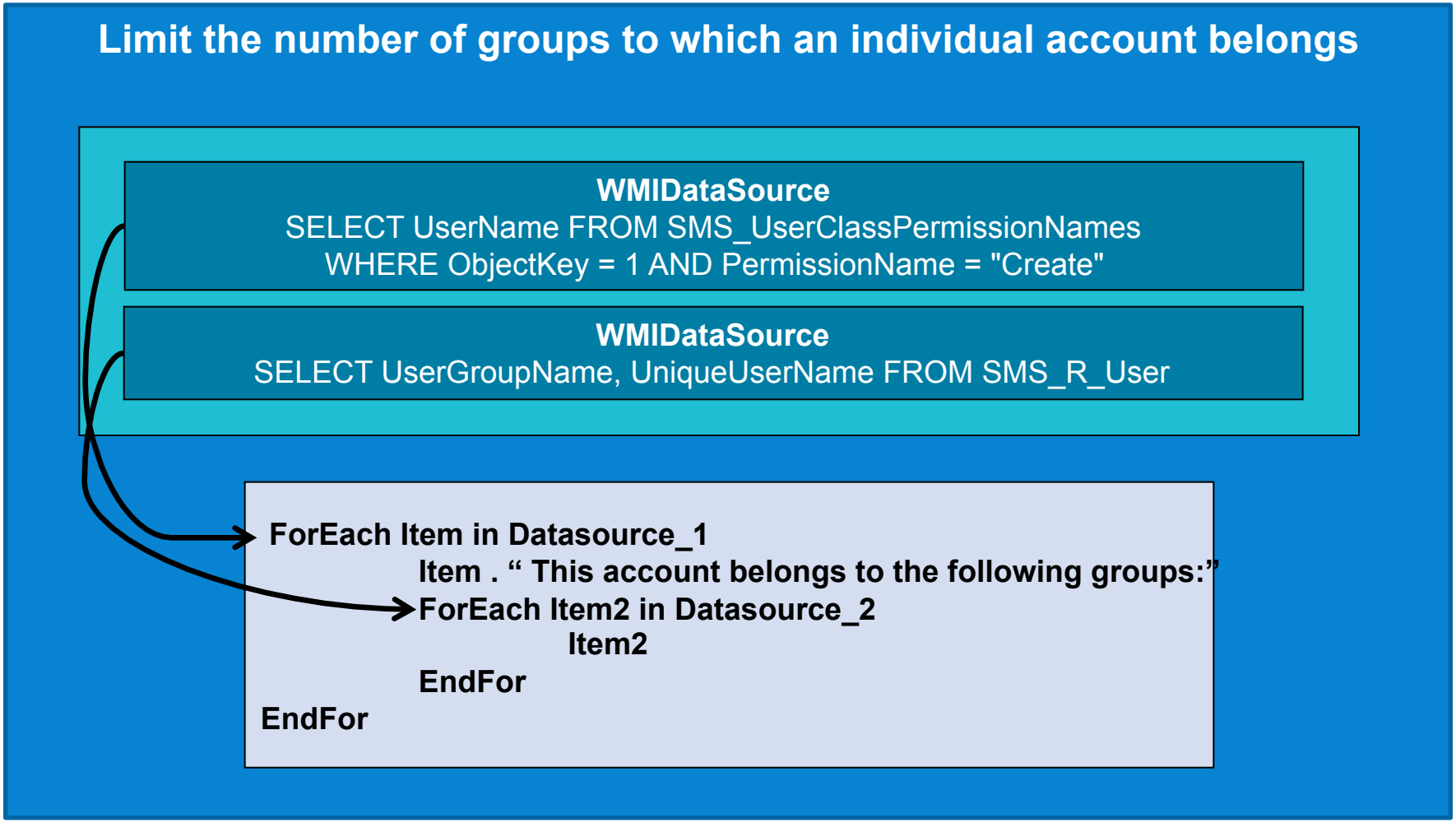
http://ocrl.mitre.org/

OCRL Report Definition Structure

- Schema is currently a proof-of-concept
- ReportDefinition has two parts – DataSources and Reporting
- DataSources
  - Gather state from system repositories
  - Different subclasses for different repositories (like OVAL)
  - Experiment using reference to OVAL Object structures
- Reporting
  - Controls the organization of the collected data in the report



OCRL Example



OCRL Example Output

Recommendation: Limit the number of groups to which an individual account belongs

****

Instructions: Review the following account information to decide whether changes are needed for compliance with the recommendation:

UserName: Lisa
This account belongs to the following groups:
UserGroupName: Admins
UserGroupName: Administrator

UserName: Len
This account belongs to the following groups:
UserGroupName: Administrator
UserGroupName: SMS Operator

UserName: Charles
This account belongs to the following groups:

UserName: Shaan
This account belongs to the following groups:

UserName: Linda
This account belongs to the following groups:

OCRL Use Case

- Information exists on a system and is accessible, but automatic evaluation is not possible
  - Criteria for evaluation requires human knowledge
    - "Are all these enabled services necessary?"
    - Report shows a list of currently enabled services
  - Evaluation requires cross referencing multiple data sources
    - "Does any user have access to both key A and key B? (Ensure 2-person access)"
    - Report shows a list of users and their key lists
      - Evaluation would be impossible in OVAL if data was stored by key
- OCRL allows compilation of (potentially diverse) data sets and formatting them in a way that a user can quickly use them to determine compliance
  - Report can be called from XCCDF, but always returns "INFORMATIONAL"

OCRL Use Case Discussion

- MITRE has experienced cases where this capability would be useful
  - Grant access privileges to the ITIM_HOME directory and its subdirectories only to users who require access.
    - Gather user privilege data, display report to admin, admin decides if the users require access
  - Ensure an appropriate value for the recycle bin retention period is set based on available disk space.
    - Gather recycle bin retention periods, display report to admin, admin decides if it is appropriate
- Does the community see a need for this use case?
- Should we be using a new or existing spec?