# Usable Security for Security Professionals

**Pooya Jaferian**

Laboratory for Education and Research in Secure Systems Engineering (LERSSE)

University of British Columbia, Vancouver, Canada

# Agenda

- Background
- Guidelines and heuristics for IT security tools
- Field study of Identity and Access Management
- Improving access certification interfaces
- Future work

# BACKGROUND

# Background

Pooya Jaferian

Hootan Rashtian

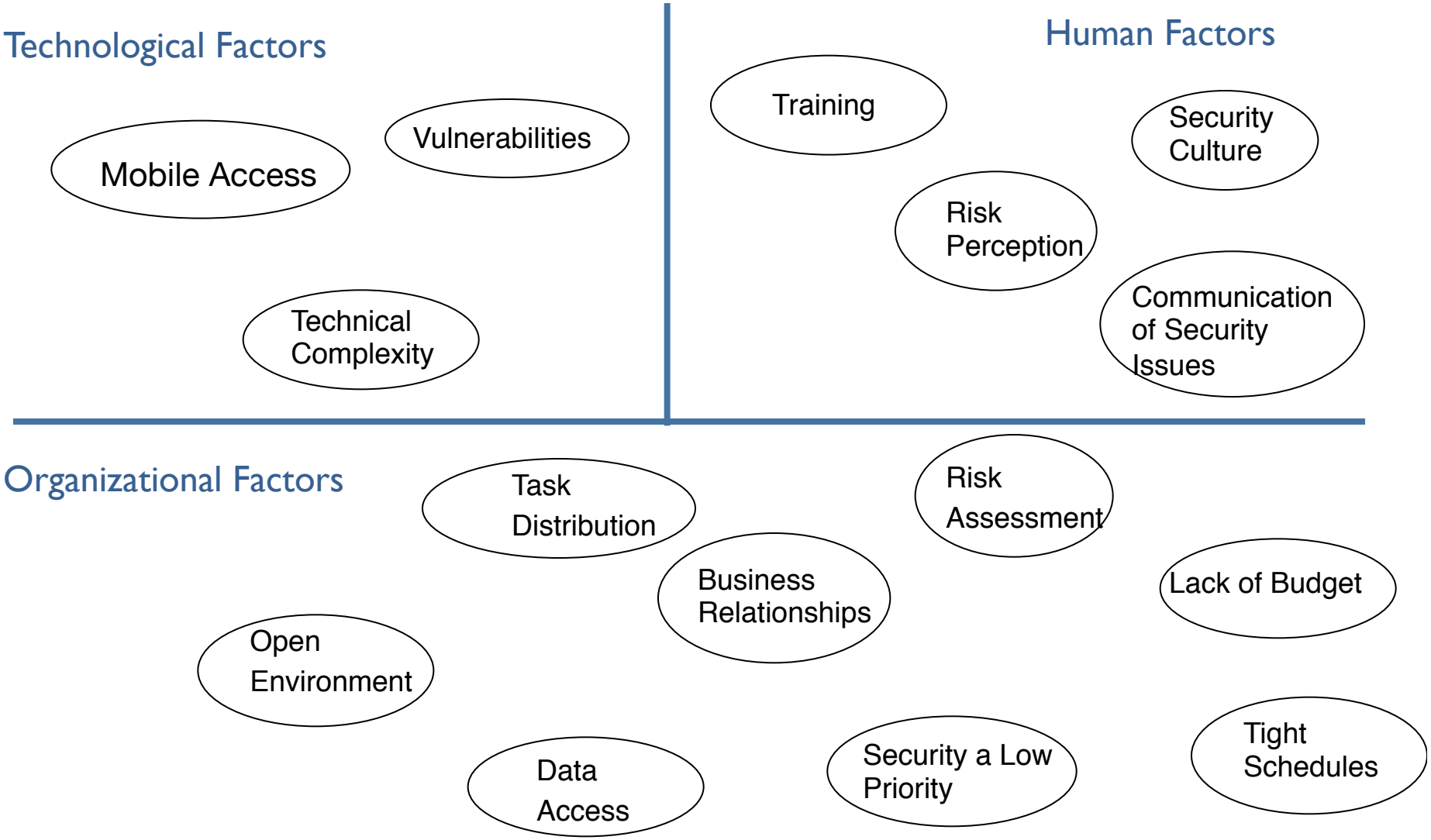
Kirstie Hawkey

Kosta Beznosov

# HOT-Admin Project

- Field study
  - 36 semi-structured interviews
  - More than 15 hours of participatory observation
- Results
  - Tasks and Tools
  - IT Security vs. IT
  - Challenges in ITSM (IT Security Management)
  - Interactions and Collaboration in ITSM
  - Sub-optimal situations in ITSM
  - Diagnostic Work in ITSM
  - Guidelines for ITSM tools

# IT security challenges



# Characteristics of IT security domain

- Technological complexity
- Collaboration
- Stakeholder diversity

# Characteristics of IT security domain

- Technological complexity
- Collaboration
- Stakeholder diversity

Usable tools can help security professionals dealing with these three factors

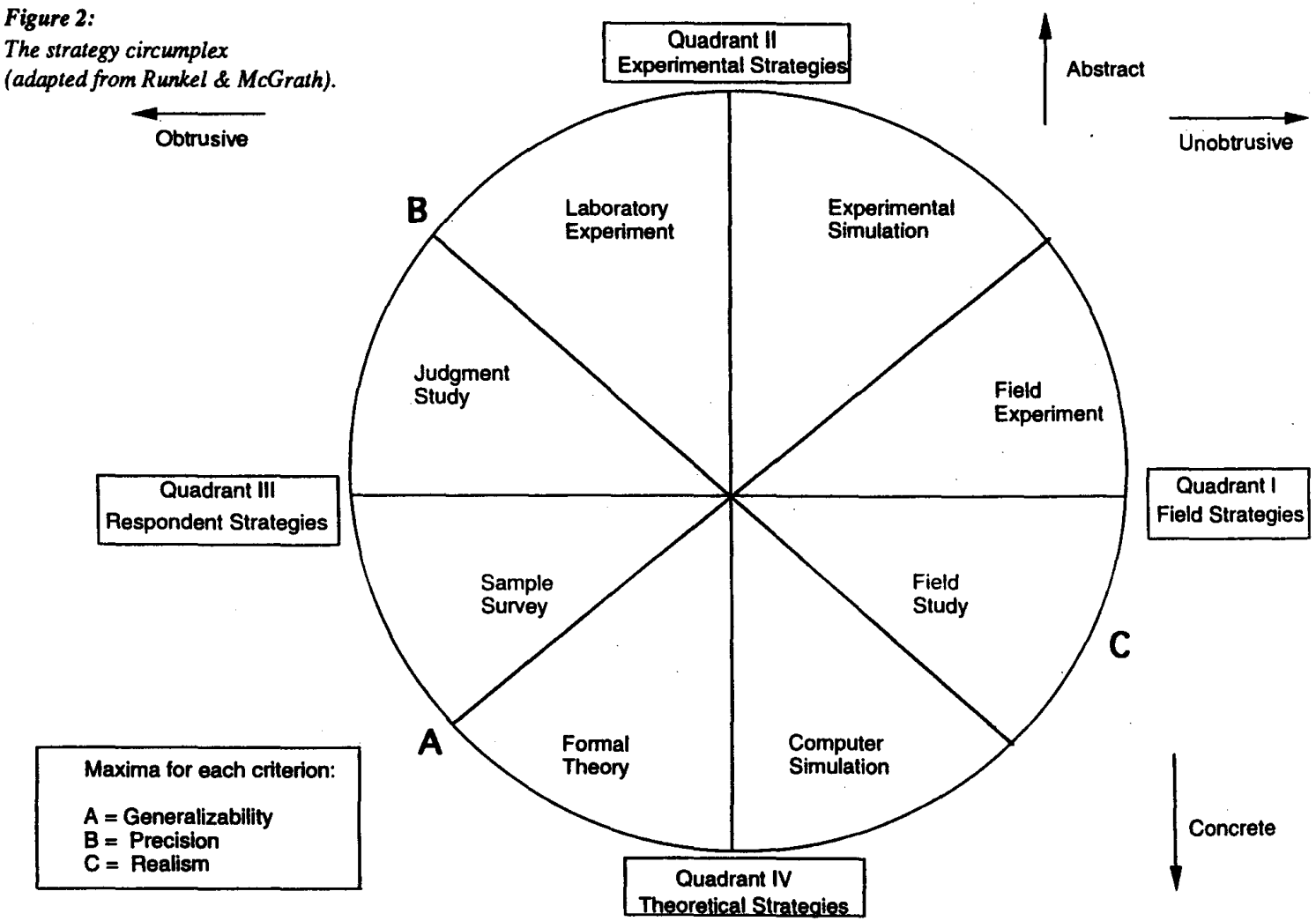
# Challenges of studying usability of IT security tools

- Recruitment
- Actions are distributed over time and space
- Collaboration
- Technology acquisition

# HOT-IdM Project

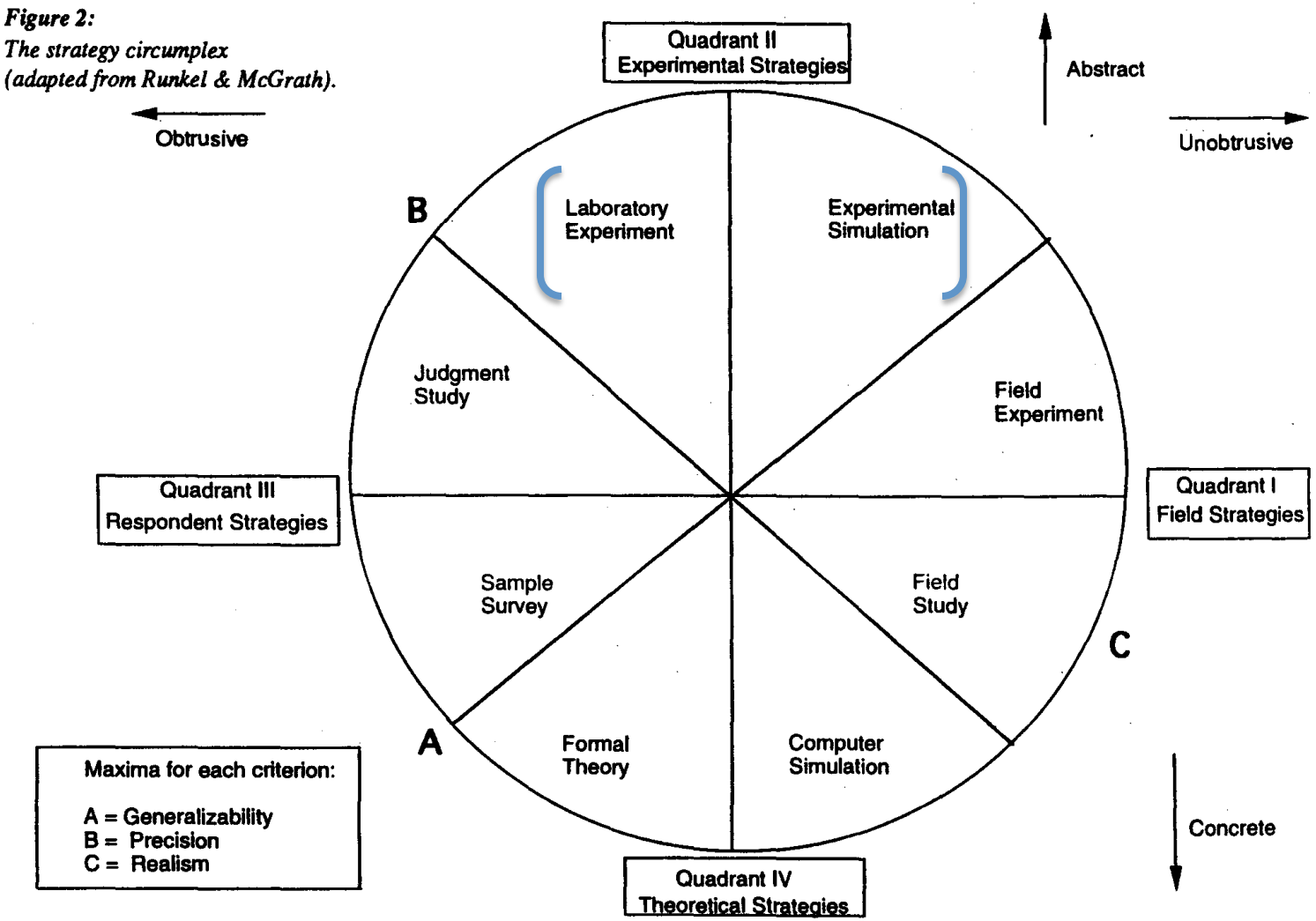
- Supported by CA and NSERC
- Project Goals:
  - "to further the understanding of the human, organizational, and technological factors influencing the effectiveness of IdM tools and processes within the context of organizations where they are employed"
  - "investigate refinements to the IdM tools in order to better support those organizations that employ them and the IT professionals who operate and manage them"

# Strategies for HCI studies



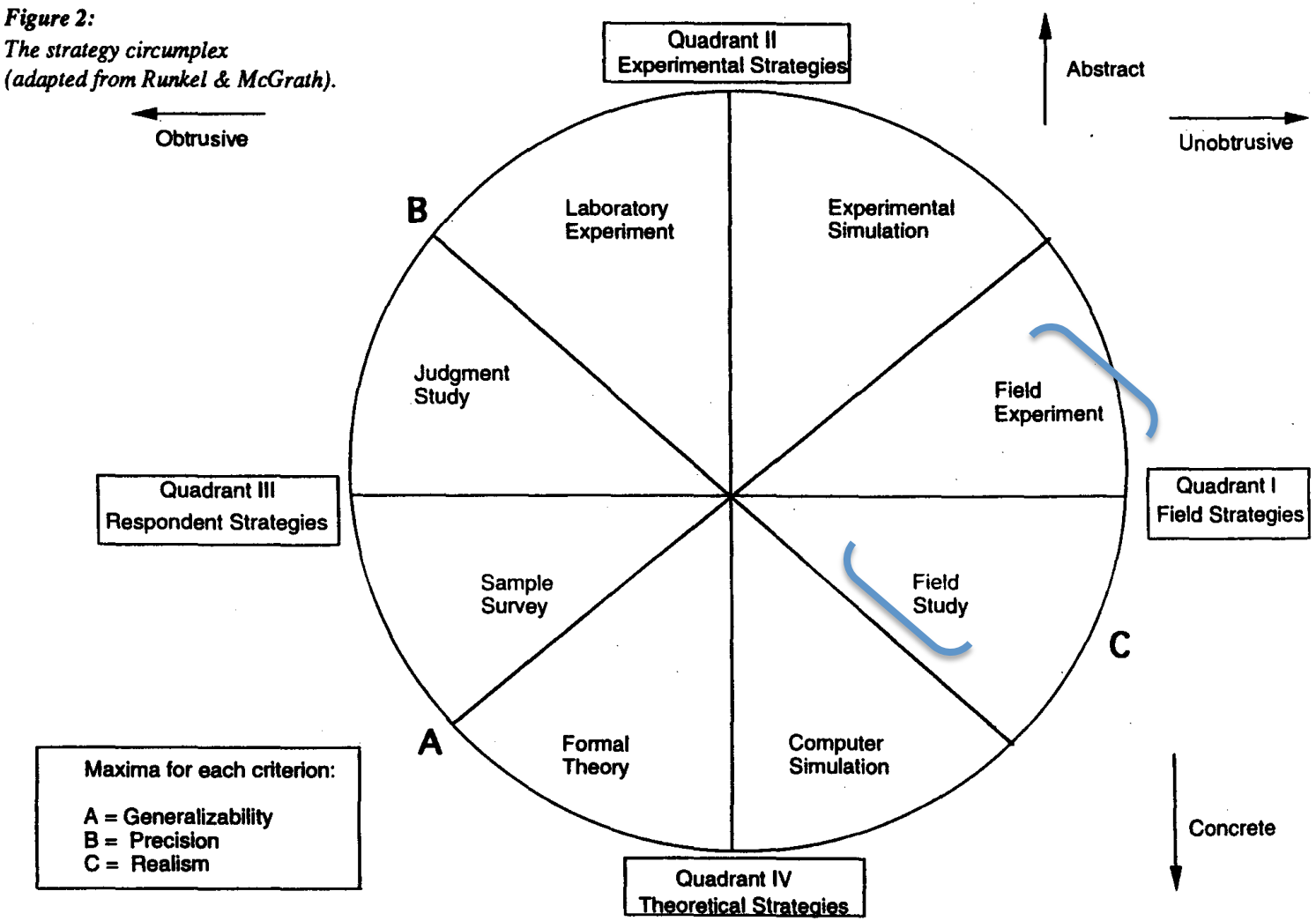

Methodology Matters: Doing Research in the Social and Behavioral Sciences
Joseph E. McGrath

# Strategies for HCI studies



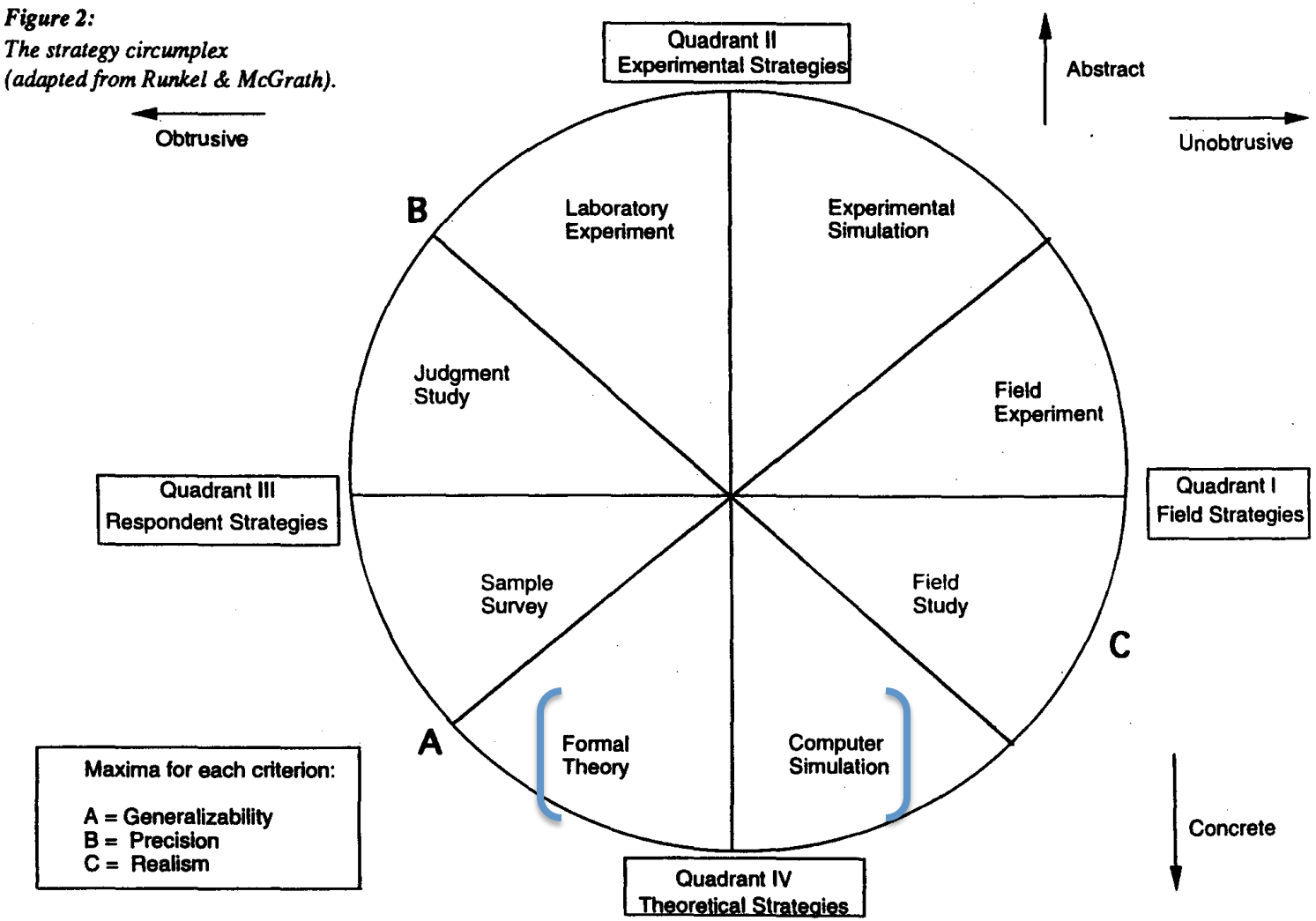

Methodology Matters: Doing Research in the Social and Behavioral Sciences
Joseph E. McGrath

# Strategies for HCI studies



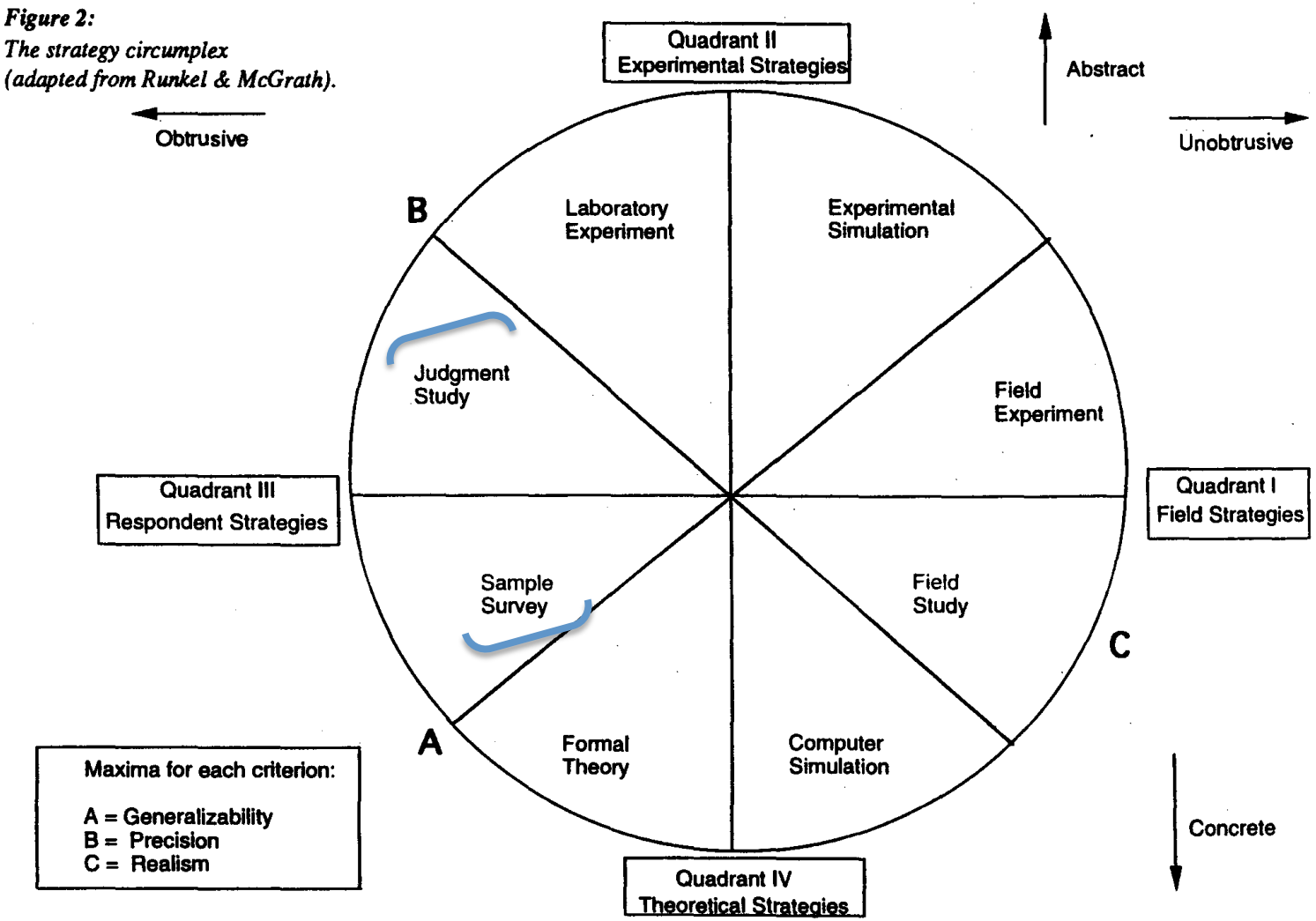

Methodology Matters: Doing Research in the Social and Behavioral Sciences
Joseph E. McGrath

# Strategies for HCI studies



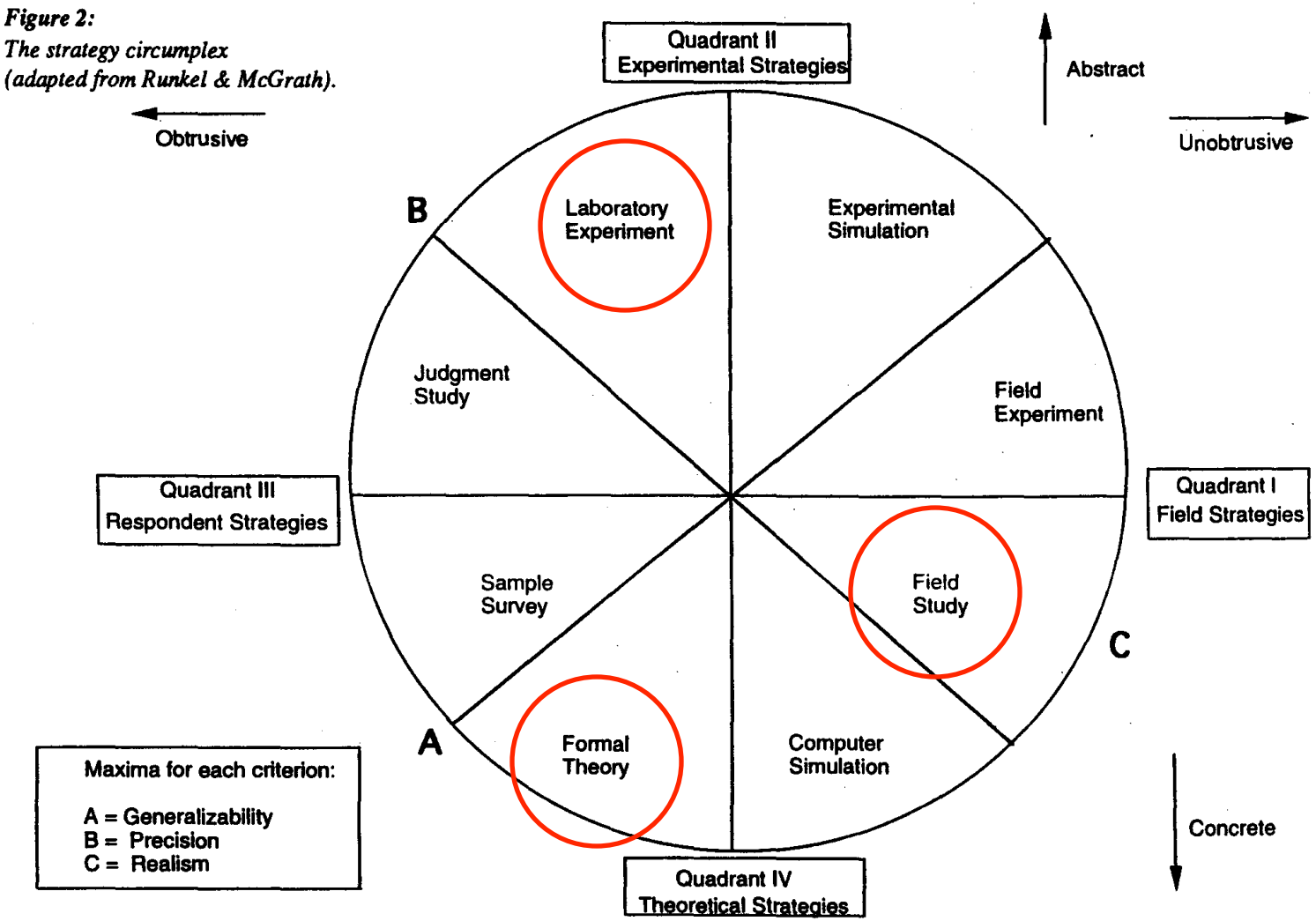

Methodology Matters: Doing Research in the Social and Behavioral Sciences
Joseph E. McGrath

# Strategies for HCI studies




Methodology Matters: Doing Research in the Social and Behavioral Sciences
Joseph E. McGrath

# Strategies for HCI studies

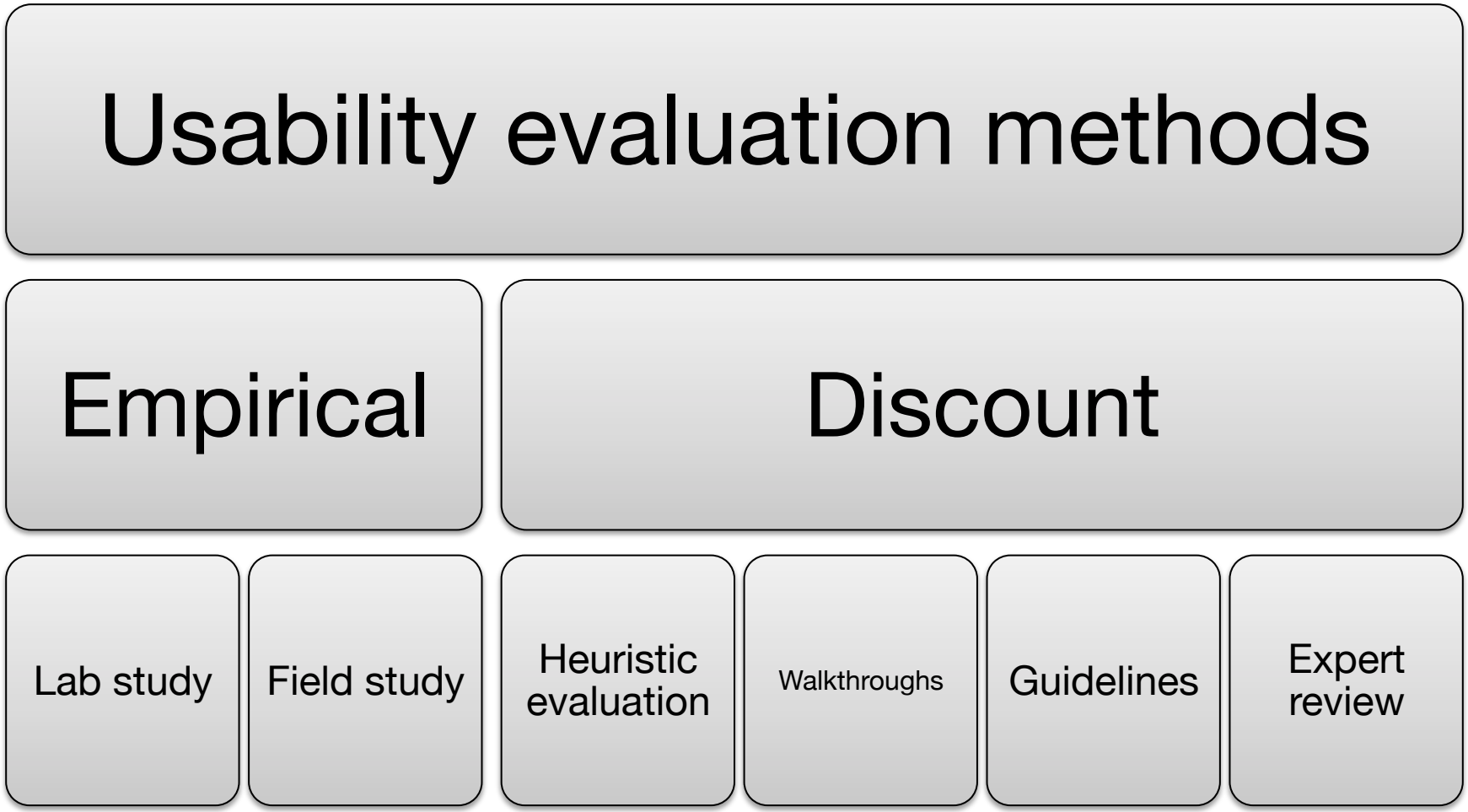



Methodology Matters: Doing Research in the Social and Behavioral Sciences
Joseph E. McGrath

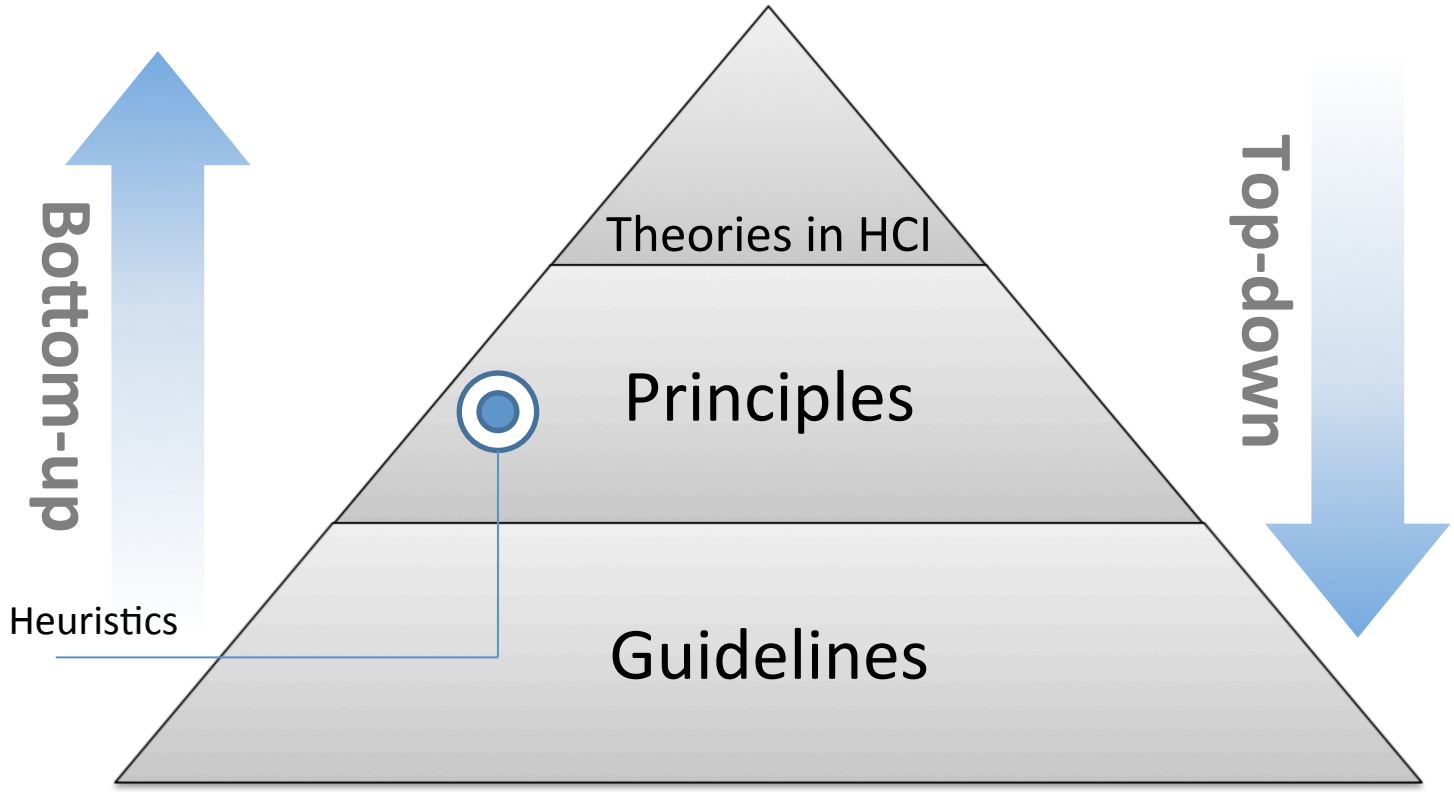
# GUIDELINES AND HEURISTICS

For usability evaluation of IT security management tools

# Usability evaluation methods



# Background: Guidance for design in HCI




Shneiderman, B. 1997 *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. 3rd. Addison-Wesley Longman Publishing Co., Inc.

# Heuristics vs. Guidelines

## Nielsen's heuristics

1. Visibility of system status
2. Match between system and the real world
3. User control and freedom
4. Consistency and standards
5. Error prevention
6. Recognition rather than recall
7. Flexibility and efficiency of use
8. Aesthetic and minimalist design
9. Help users recognize, diagnose, and recover from errors
10. Help and documentation

Source: www.useit.com

## iOS Location Services and Data Privacy guidelines

1. Make sure users understand why they're being asked to share their personal data
2. Describe why your app needs the information, if it's not obvious
3. Ask permission at app startup only if your app can't perform its primary function without the user's data
4. Avoid making programmatic calls that trigger the alert before the user actually selects the feature that needs the data
5. For location data, check the Location Services preference to avoid triggering the alert unnecessarily

Source: www.apple.com

# Heuristics vs. Guidelines

## Principles for Secure Systems

1. Path of Least Resistance
2. Active Authorization
3. Revocability
4. Visibility
5. Self-Awareness
6. Trusted Path
7. Expressiveness
8. Relevant Boundaries
9. Identifiability
10. Foresight

(Yee 2002)

## iOS Location Services and Data Privacy guidelines

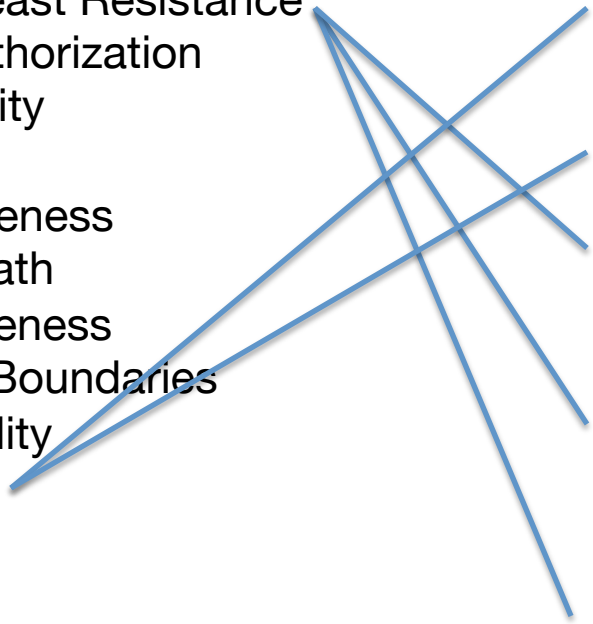
1. Make sure users understand why they're being asked to share their personal data
2. Describe why your app needs the information, if it's not obvious
3. Ask permission at app startup only if your app can't perform its primary function without the user's data
4. Avoid making programmatic calls that trigger the alert before the user actually selects the feature that needs the data
5. For location data, check the Location Services preference to avoid triggering the alert unnecessarily

Source: www.apple.com

# Heuristics vs. Guidelines

**Principles for Secure Systems**

1. Path of Least Resistance
2. Active Authorization
3. Revocability
4. Visibility
5. Self-Awareness
6. Trusted Path
7. Expressiveness
8. Relevant Boundaries
9. Identifiability
10. Foresight



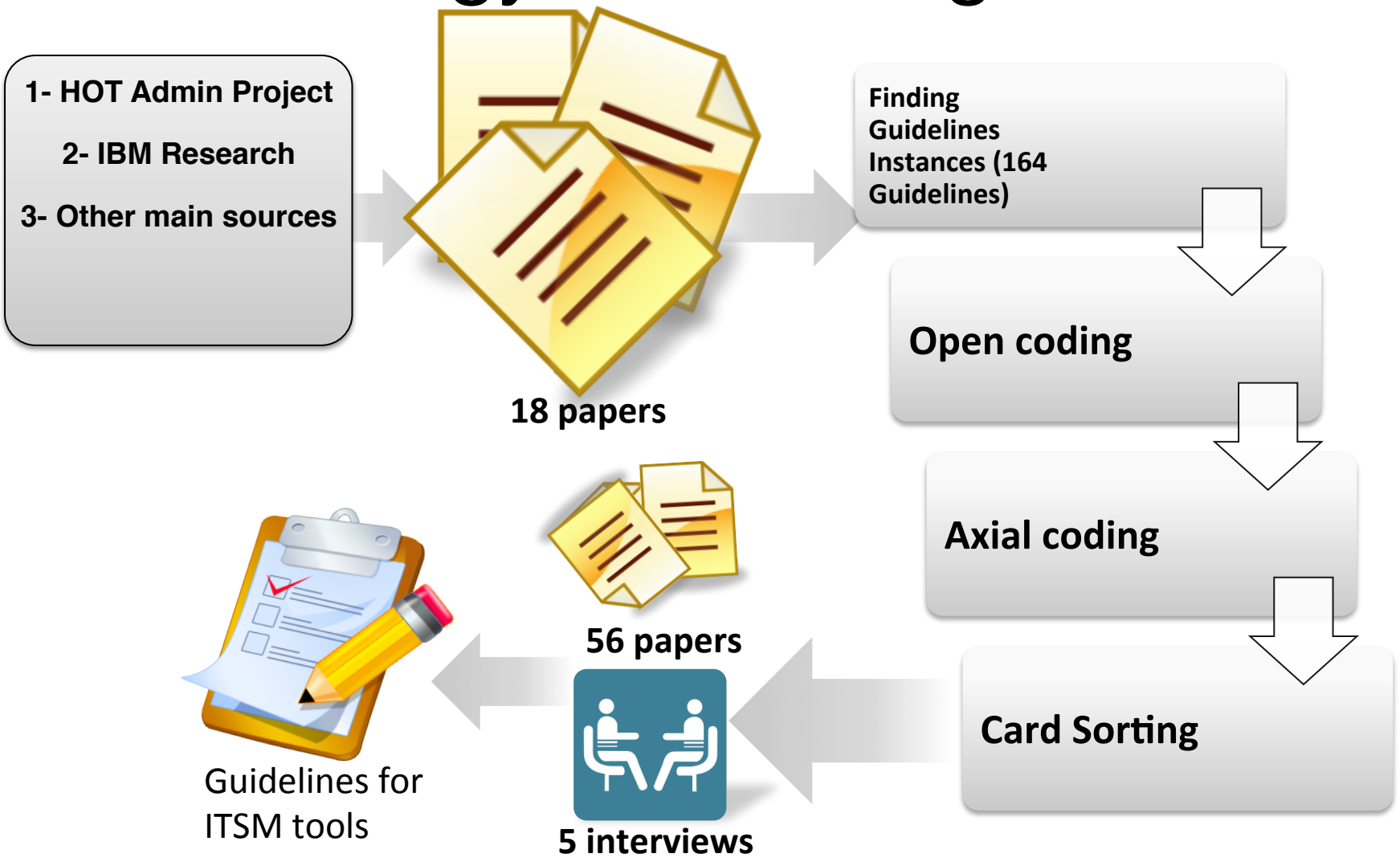
**iOS Location Services and Data Privacy guidelines**

1. Make sure users understand why they're being asked to share their personal data
2. Describe why your app needs the information, if it's not obvious
3. Ask permission at app startup only if your app can't perform its primary function without the user's data
4. Avoid making programmatic calls that trigger the alert before the user actually selects the feature that needs the data
5. For location data, check the Location Services preference to avoid triggering the alert unnecessarily

(Yee 2002)

Source: www.apple.com

# Methodology for building heuristics

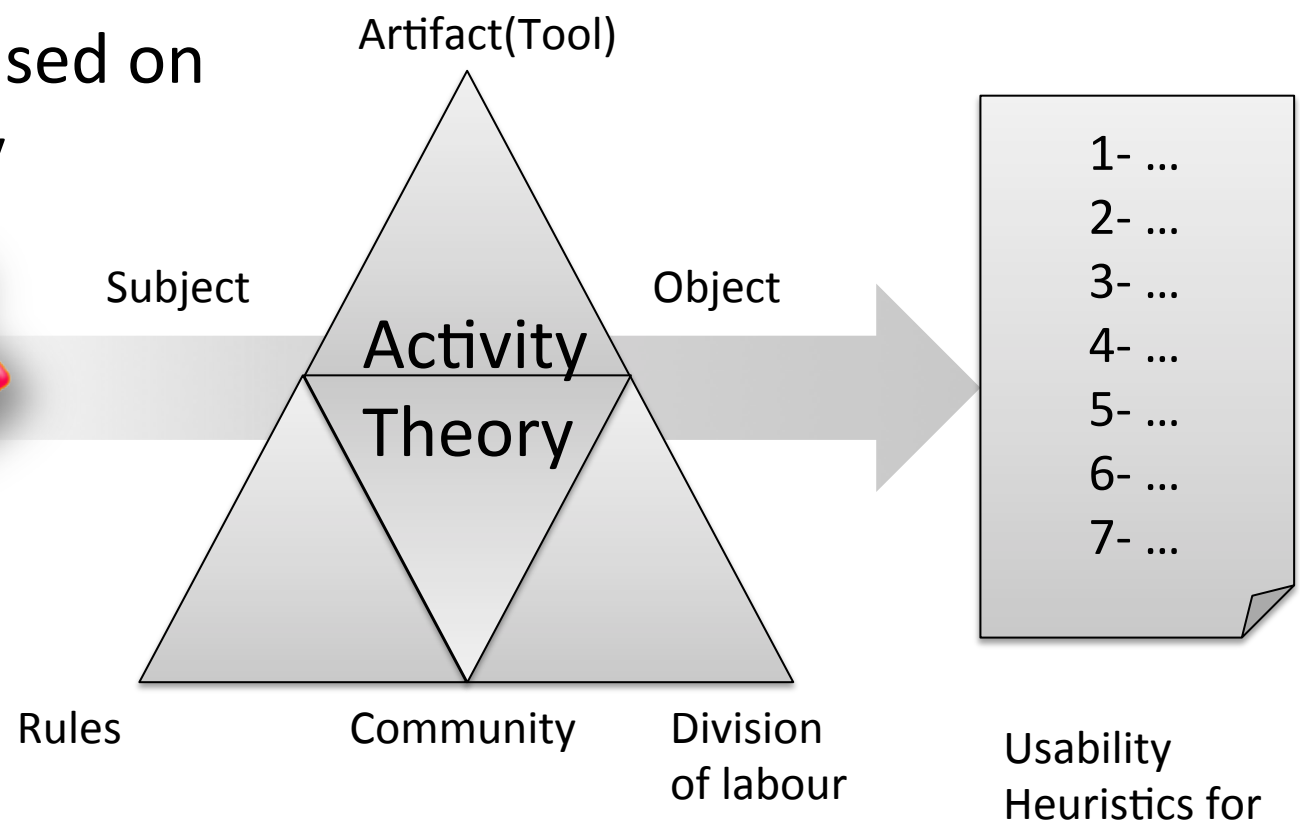



P. Jaferian, D. Botta, F. Raja, K. Hawkey, and K. Beznosov. 2008. Guidelines for designing IT security management tools. In CHiMiT '08.

# Interpretation of Guidelines based on Activity Theory

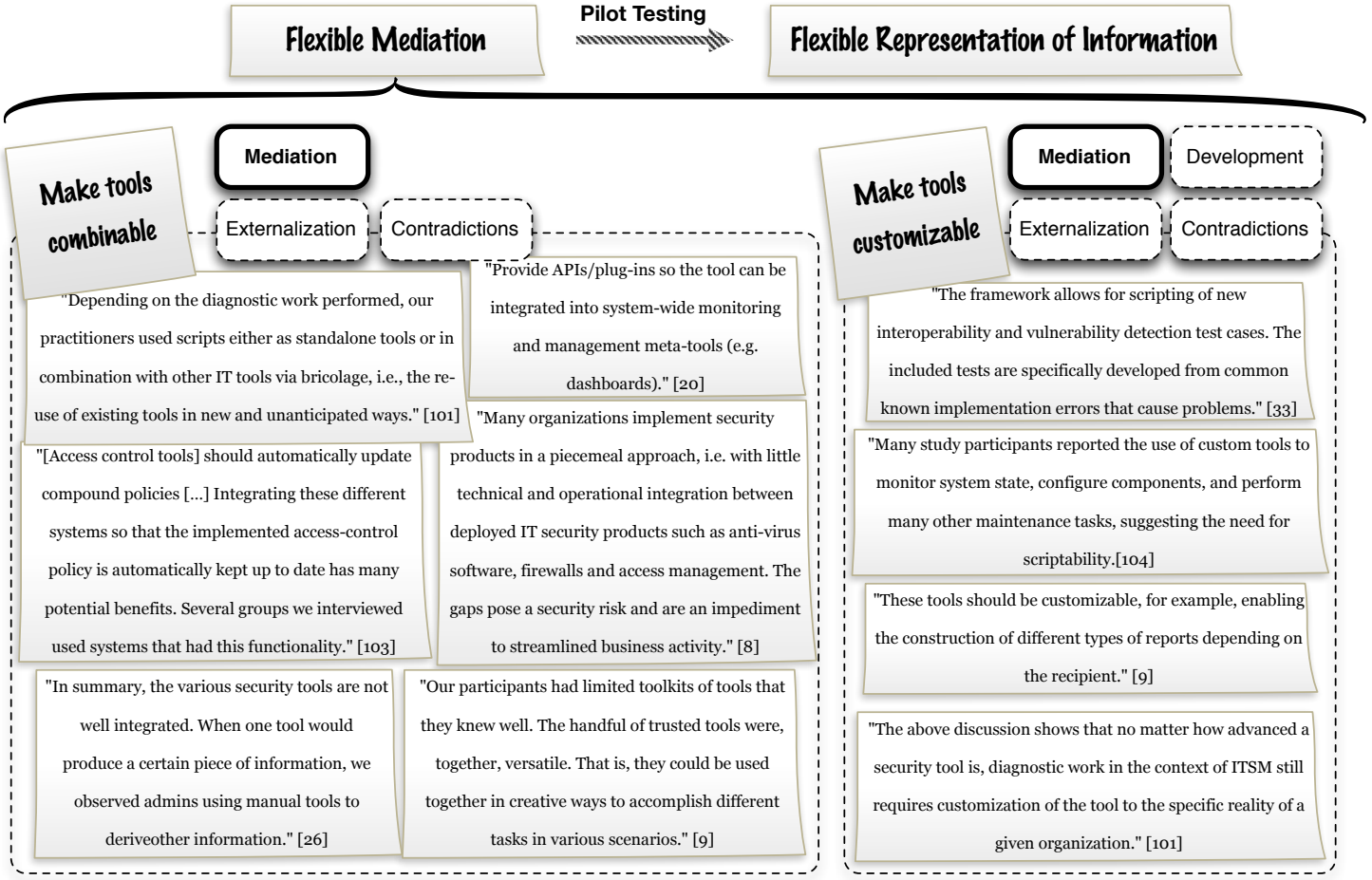
Interpretation and abstraction based on activity theory

Guidelines for ITSM tools




Usability Heuristics for ITSM tools

# Example of Heuristic Synthesis



# ITSM Usability heuristics

- *1- Visibility of activity status*
- *2- History of actions and changes on artefacts*
- *3- Flexible representation of information*
- *4- Rules and constraints*
- *5- Planning and dividing work between users*
- *6- Capturing, sharing, and discovery of knowledge*
- *7- Verification of knowledge*

# ITSM Usability heuristics

- *1- Visibility of activity status*
- *2- History of actions and changes on artefacts*

***Allow capturing the history of actions and changes on tools or other artefacts such as policies, logs, and communications between users. Provide a means for searching and analyzing historical information.***

Evaluation of CA Identity Manager

# COMPARING NIELSEN AND ITSM HEURISTICS

# Study Goals

- Compare the use of ITSM and Nielsen's heuristics
- Find usability problems in CA identity manager

# Study Goals

Independent Variables → Dependent Variables:

What you change in the study

What is expected to change when you change independent variable

# Study Goals

Independent Variables
Heuristic Set
- ITSM
- Nielsen

Dependent Variables:
Number of problems
Severity of problems

# Between vs. Within Subjects

- Each participant is used once
- Each participant is used multiple times

# Between vs. Within Subjects

- Each participant is used once
- Large number of participants
- Assignment bias
- High variability

- Each participant is used multiple times
- Carryover effect
  - Learning
  - Fatigue
- Long evaluation sessions

# Study Design

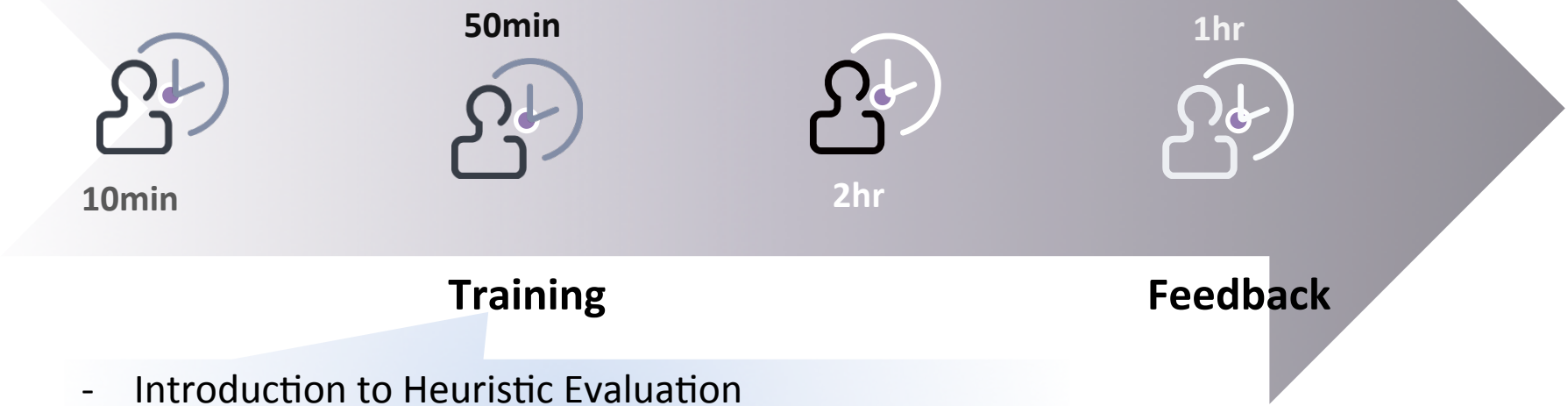
- A between subjects study with two conditions (ITSM, and Nielsen)
- 14 participants in each condition
- Participants had prior HCI training and heuristic evaluation experience
- CA Identity Manager R12.0 CR3

# Comparative Study of ITSM and Nielsen's Heuristics

- Four scenarios
- Evaluators specified problem, and the heuristic(s) using which they found the problem

**Consent and background questionnaire**

**Evaluation**




**Training**

**Feedback**

- Introduction to Heuristic Evaluation
- Overview on the heuristics (Nielsen or ITSM)
- Examples of applying the heuristics on an IDS
- Introduction to the IdM system and a system demo

# Data Analysis

Problem Synthesis

- Decompose problems, marking false positives and unknowns

Aggregating problems

- Combining similar problems by different evaluators

Tagging problems

- Mapping problems to heuristics

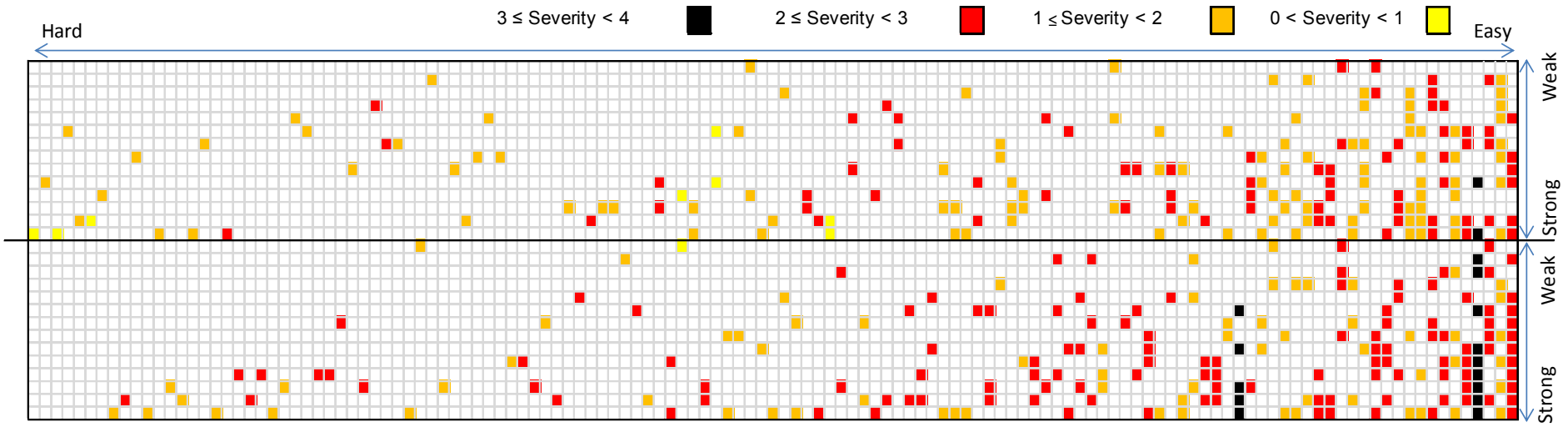
Rating Severity

- Rating severity (1—5)

# Overview of Results

| Condition | Reports | Tokens | Known | Major | Minor | FP | Unknown |
|---|---|---|---|---|---|---|---|
| ITSM | 239 | 201 | 93 77% | 38 | 55 | 18 | 16 |
| Nielsen | 233 | 187 | 86 60% | 20 | 66 | 45 | 17 |
| All | 472 | 388 | 131 | 37 | 94 | 62 | 33 |

# Comparing individual differences



# Summary of findings

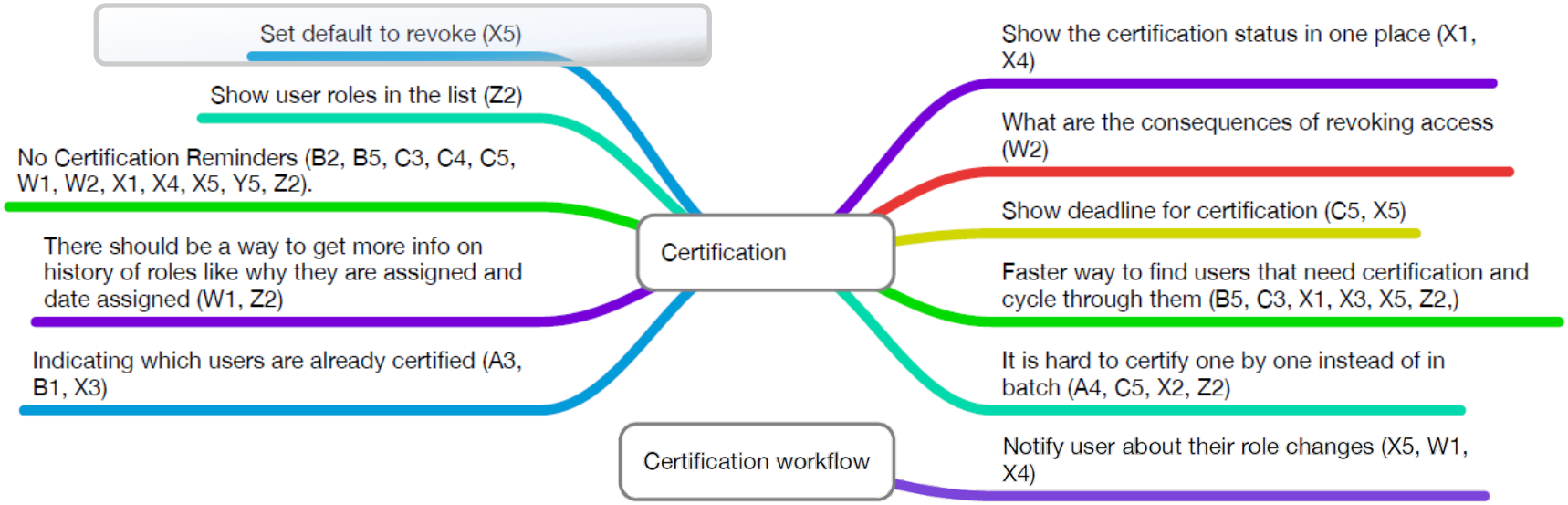
- Severity of the problems found by individual evaluators in ITSM condition is higher than Nielsen condition.
- Participants found the ITSM heuristics to be as relevant, easy to apply, and easy to learn as Nielsen's heuristics.
- Evaluating the IdM system heuristically, required more effort compared to previous evaluations.
- We suggest using both ITSM and Nielsen’s heuristics.

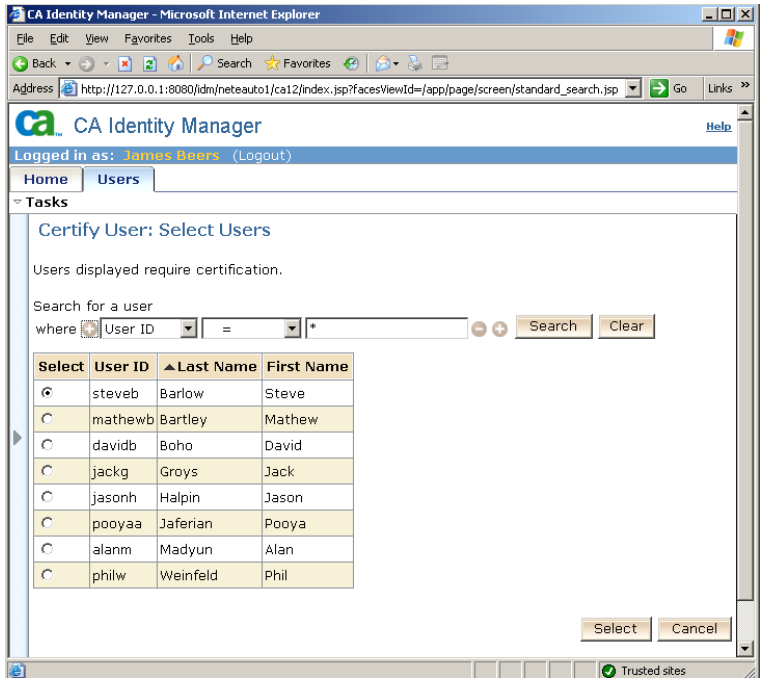
Access Certification

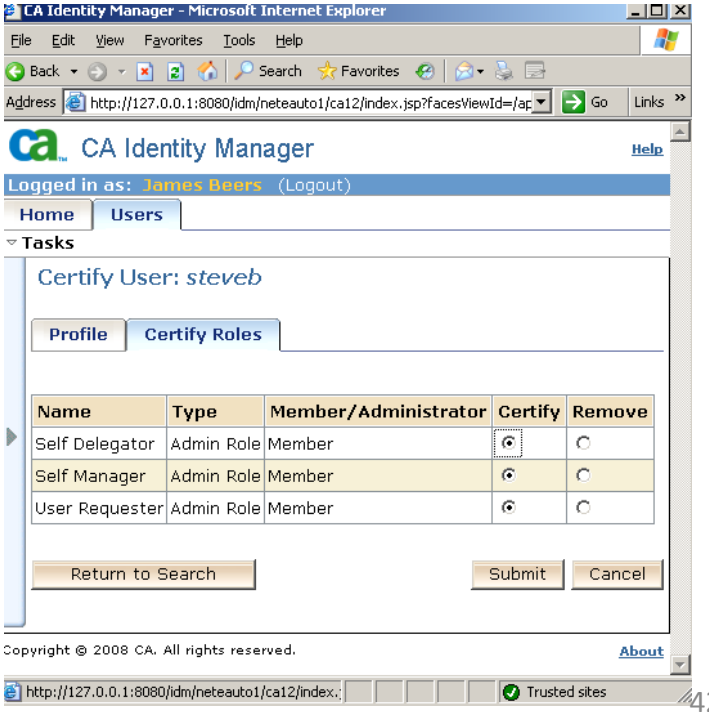
# PROBLEMS FOUND THROUGH HEURISTIC EVALUATION

# Introduction

- Heuristic evaluation for 4 scenarios:
  - Self-serve account creation
  - Bulk loader
  - Role request
  - Certification
- Participants codes:
  - A, B, C: Nielsen
  - W, X, Y, Z: ITSM


Set default to revoke (X5)
Show user roles in the list (Z2)
No Certification Reminders (B2, B5, C3, C4, C5, W1, W2, X1, X4, X5, Y5, Z2).
There should be a way to get more info on history of roles like why they are assigned and date assigned (W1, Z2)
Indicating which users are already certified (A3, B1, X3)
Certification
Certification workflow
Show the certification status in one place (X1, X4)
What are the consequences of revoking access (W2)
Show deadline for certification (C5, X5)
Faster way to find users that need certification and cycle through them (B5, C3, X1, X3, X5, Z2,)
It is hard to certify one by one instead of in batch (A4, C5, X2, Z2)
Notify user about their role changes (X5, W1, X4)

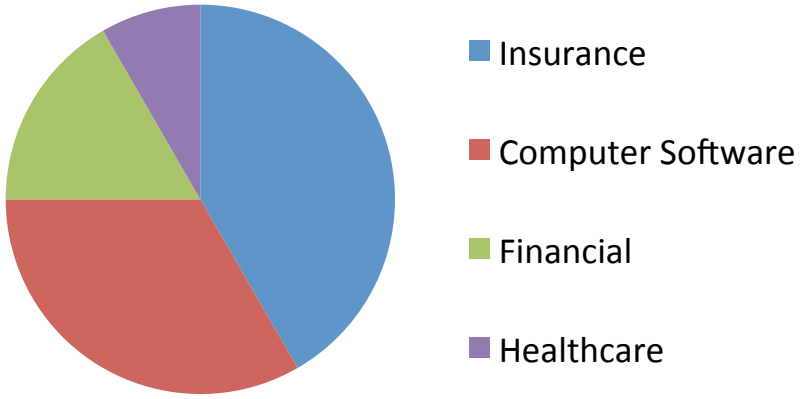

CA Identity Manager - Microsoft Internet Explorer
CA Identity Manager
Logged in as: James Beers (Logout)
Home
Users
Tasks
Certify User: Select Users
Users displayed require certification.
Search for a user
where User ID = * Search Clear
Select User ID Last Name First Name
steveb Barlow Steve
mathewb Bartley Mathew
davidb Boho David
jackg Groys Jack
jasonh Halpin Jason
pooyaa Jaferian Pooya
alanm Madyun Alan
philw Weinfeld Phil
Select Cancel


CA Identity Manager - Microsoft Internet Explorer
CA Identity Manager
Logged in as: James Beers (Logout)
Home
Users
Tasks
Certify User: steveb
Profile
Certify Roles
Name Type Member/Administrator Certify Remove
Self Delegator Admin Role Member
Self Manager Admin Role Member
User Requester Admin Role Member
Return to Search
Submit
Cancel
Copyright © 2008 CA. All rights reserved.
About

# FIELD STUDY OF IDM

# Overview

- 12 Semi-structured interviews

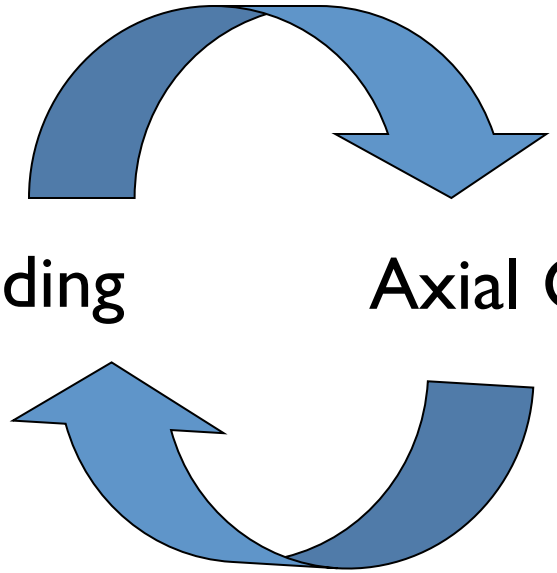



- Between one hour to three hours
- Audio recorded and transcribed
- Analyzed using grounded theory

# Qualitative analysis using grounded theory

- simultaneous collection and analysis of data
- creation of analytic codes and categories developed from data
- inductive construction of abstract categories
- theoretical sampling to refine categories
- the integration of categories into a theoretical framework.

# Data Analysis



Open Coding

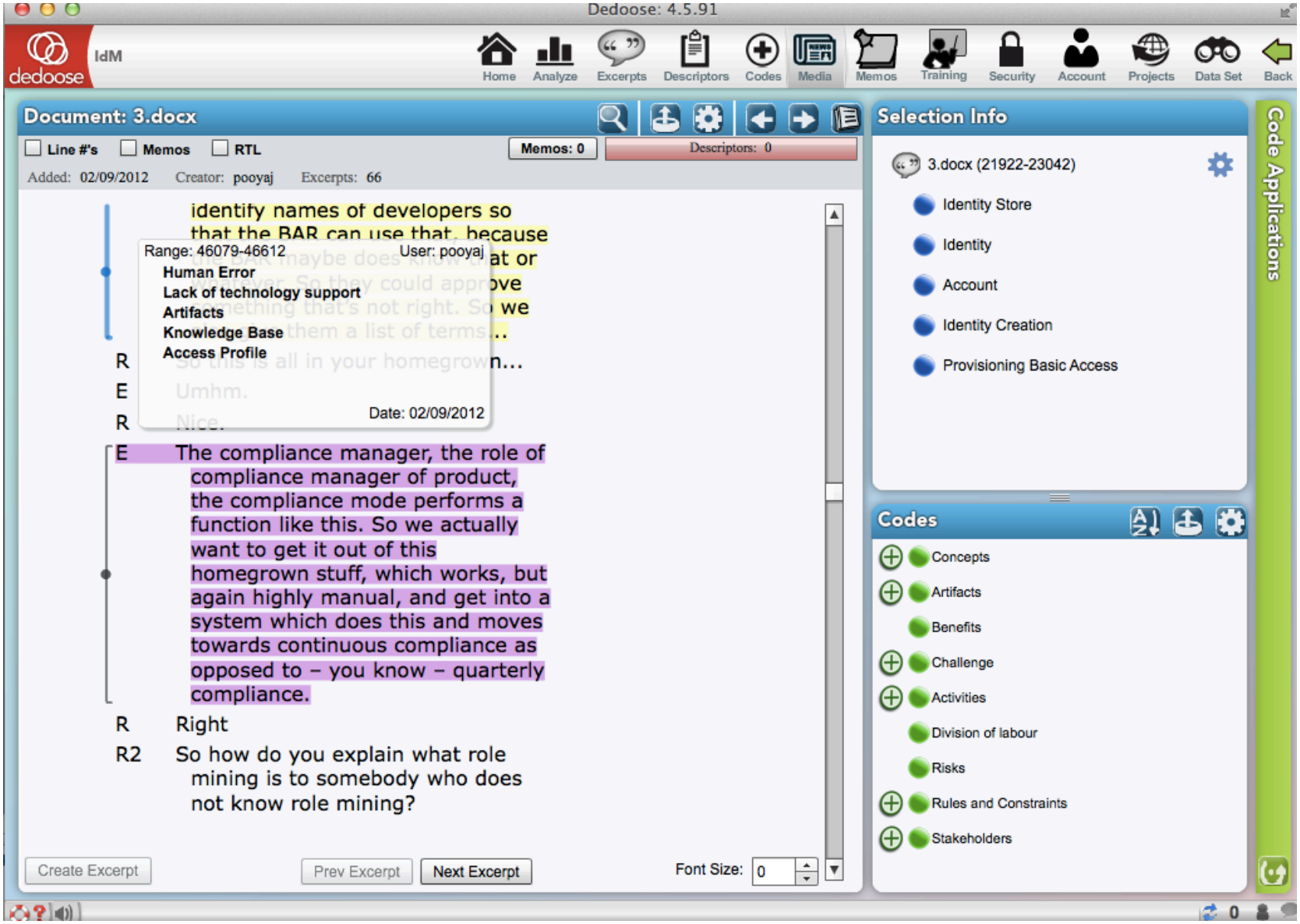
Axial Coding

selection of categories that arise from the data analysis

synthesis and refinement of the data, to make explicit the connections between the categories

# Coding Example

| Stories from Interviews | Open Codes | Axial Codes |
|---|---|---|
| "…I do my own risk assessment for everything I'm responsible for. Unfortunately in my opinion not enough people understand risk management." | Personal assessment of risk | Different perceptions of risk |
| | People do not understand risk management | |
| "in my experience these are some of the things that can happen and these are some of the potential situations you'll have to deal with" | Explain security risks | |
| "The security coordinators take it to the data guardian and explain the risks." | Explain security risks | |


Dedoose: 4.5.91
dedoose
IdM
Home
Analyze
Excerpts
Descriptors
Codes
Media
Memos
Training
Security
Account
Projects
Data Set
Back
Document: 3.docx
Line #'s
Memos
RTL
Memos: 0
Descriptors: 0
Added: 02/09/2012
Creator: pooyaj
Excerpts: 66
identify names of developers so
that the BAR can use that, because
Range: 46079-46612
User: pooyaj
Human Error
Lack of technology support
Artifacts
Knowledge Base
Access Profile
Date: 02/09/2012
R
E
R
E The compliance manager, the role of compliance manager of product, the compliance mode performs a function like this. So we actually want to get it out of this homegrown stuff, which works, but again highly manual, and get into a system which does this and moves towards continuous compliance as opposed to – you know – quarterly compliance.
R Right
R2 So how do you explain what role mining is to somebody who does not know role mining?
Create Excerpt
Prev Excerpt
Next Excerpt
Font Size:
0
Selection Info
3.docx (21922-23042)
Identity Store
Identity
Account
Identity Creation
Provisioning Basic Access
Codes
Concepts
Artifacts
Benefits
Challenge
Activities
Division of labour
Risks
Rules and Constraints
Stakeholders
Code Applications

# IdM Related Activities

1. Configuration and deployment
2. Policy creation
3. Identity creation
4. Management of identity lifecycle
5. Basic and advance provisioning and de-provisioning
6. Access certification
7. Other audit activities
8. Role engineering
9. Self-service

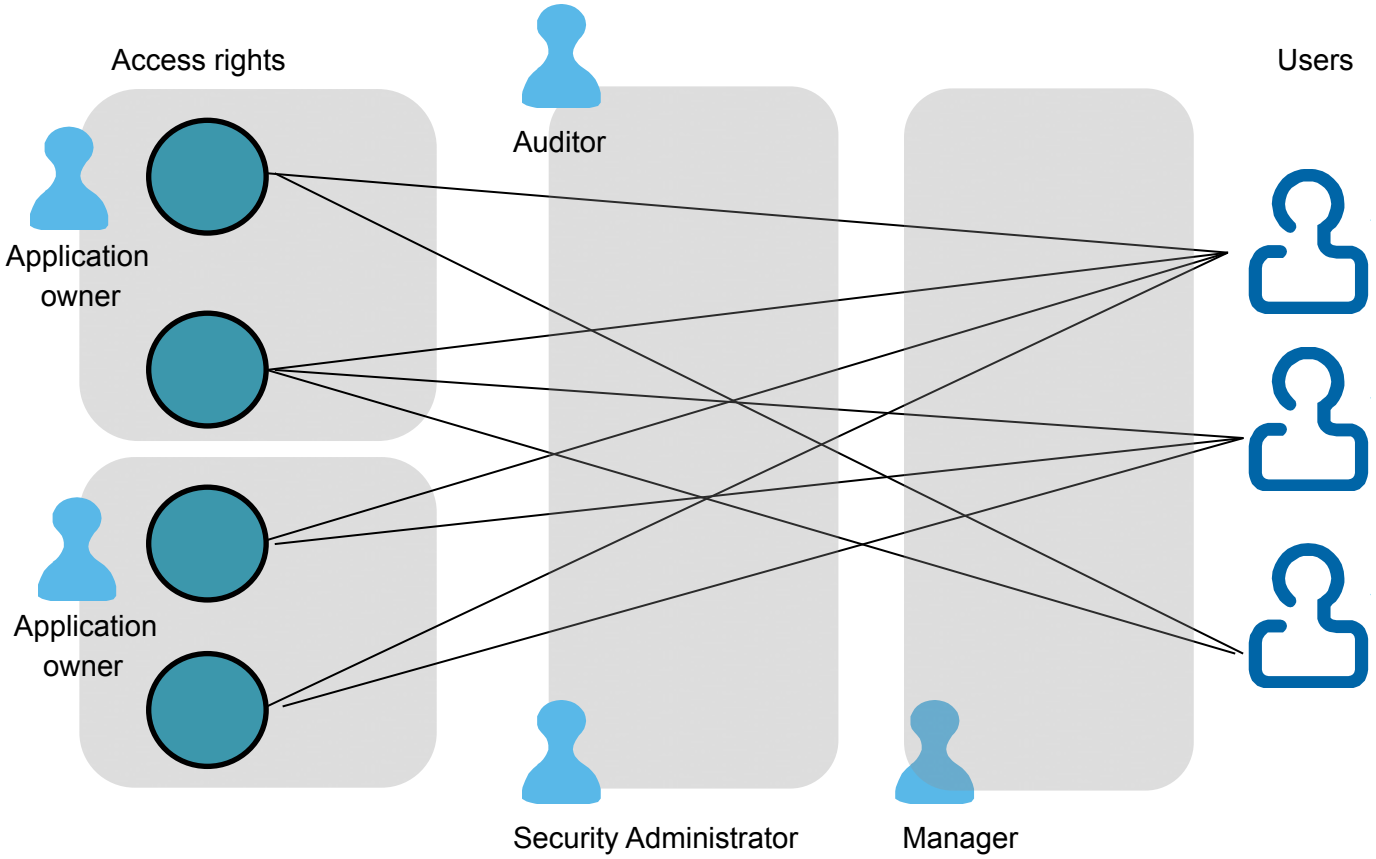
# Themes

- Actors
- Collaboration
- Artifacts
- Challenges

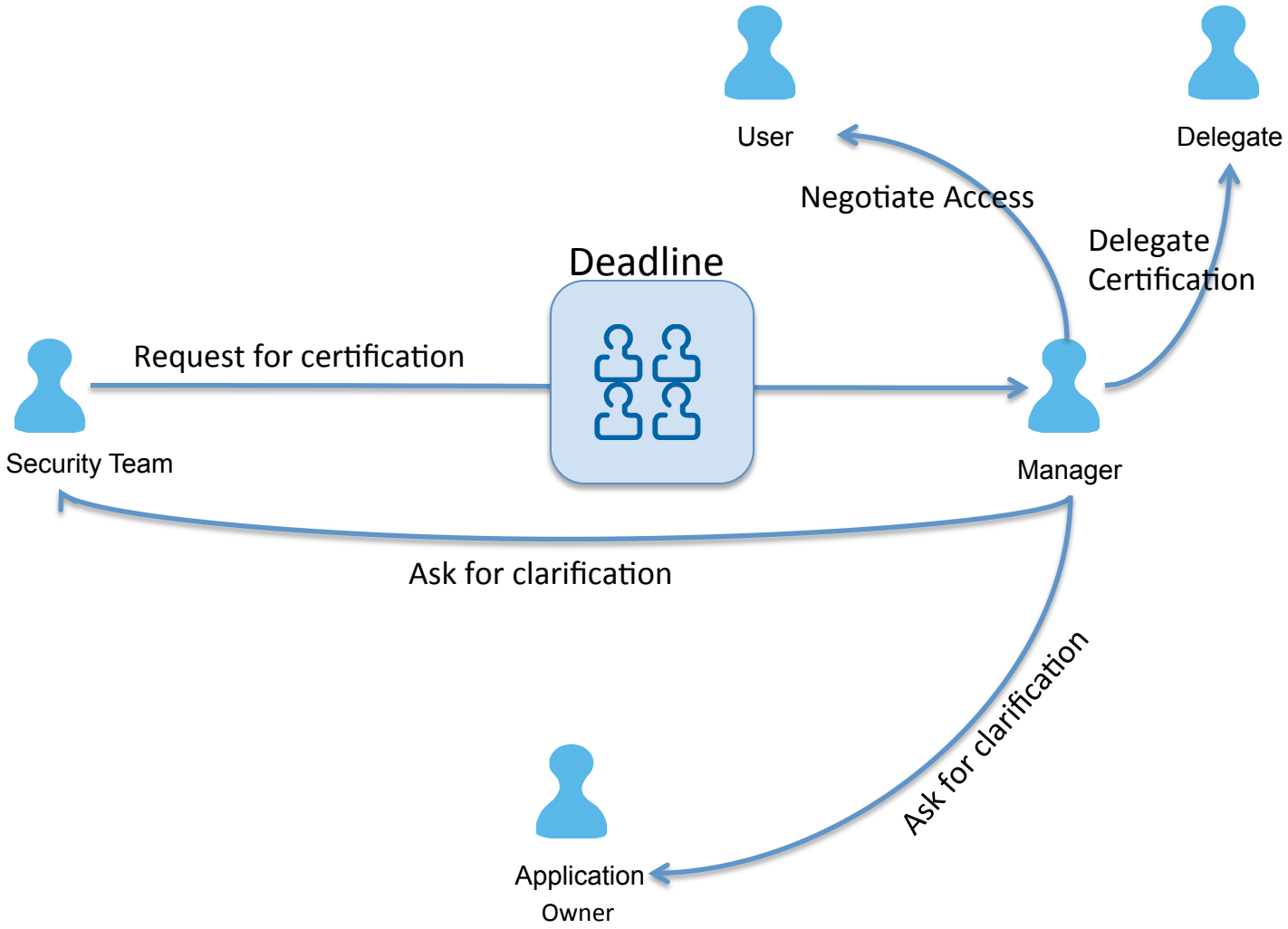
# IMPROVING USABILITY OF ACCESS CERTIFICATION INTERFACES

# Access Certification

Review of users' access rights



# Access Certification



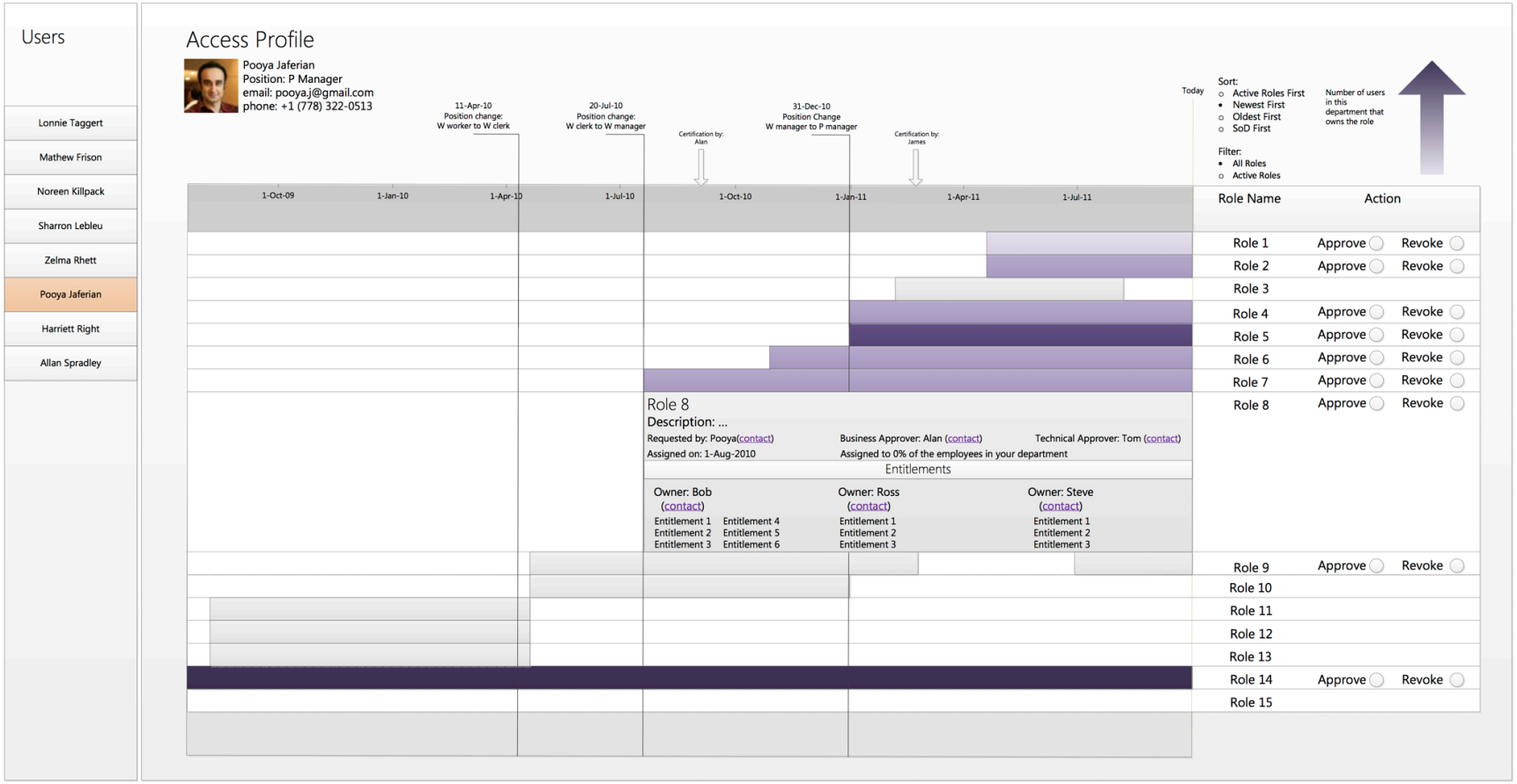
# What are the challenges?

1. Lack of understanding of access rights by managers
2. Lack of awareness about users' job function by application owners
3. Frequency (e.g., twice a year or quarterly)
4. Size of user-access rights relationships
5. Exceptional cases
6. Involves negotiation and communication

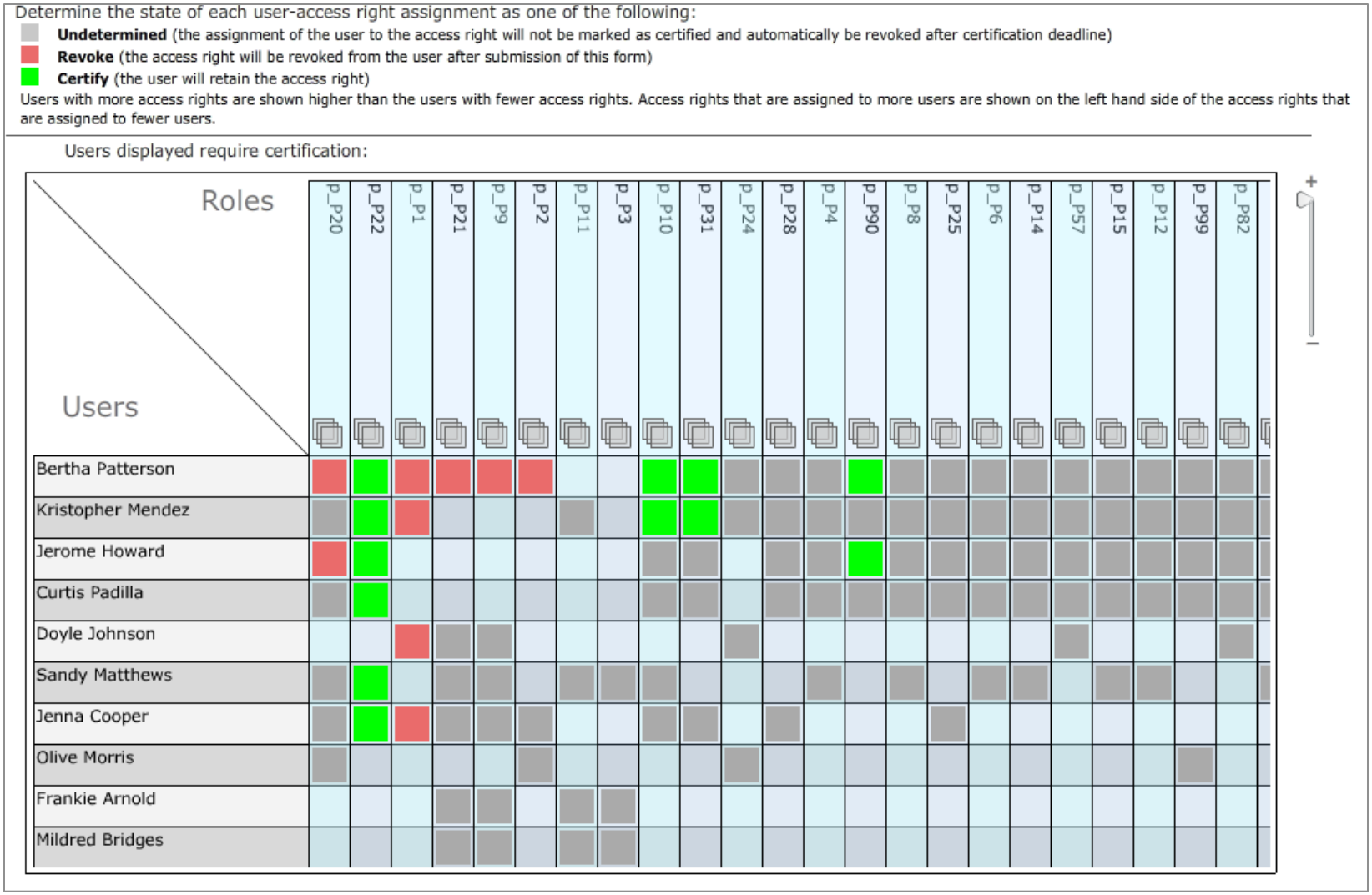
# Design Goals

- Support certification tasks
- Visibility of history
- Visibility of activity status
- Provide multiple, hierarchical views
- Provide communication and negotiation channels
- Provide risk indicators
- Highlight policy violations

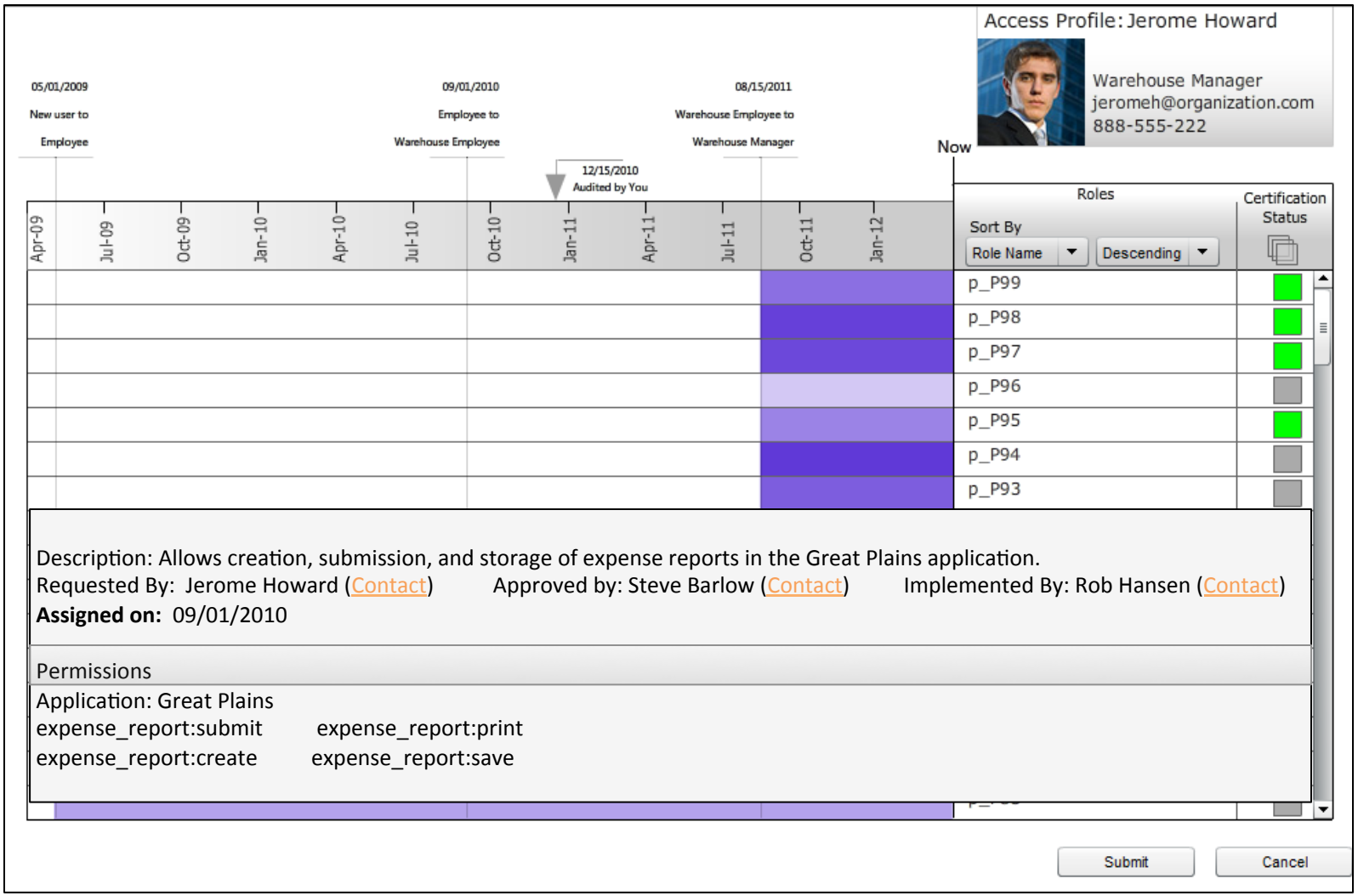
# Low-Fidelity Prototypes



# High-Fidelity Prototypes



# High-Fidelity Prototypes



# Tools for prototyping

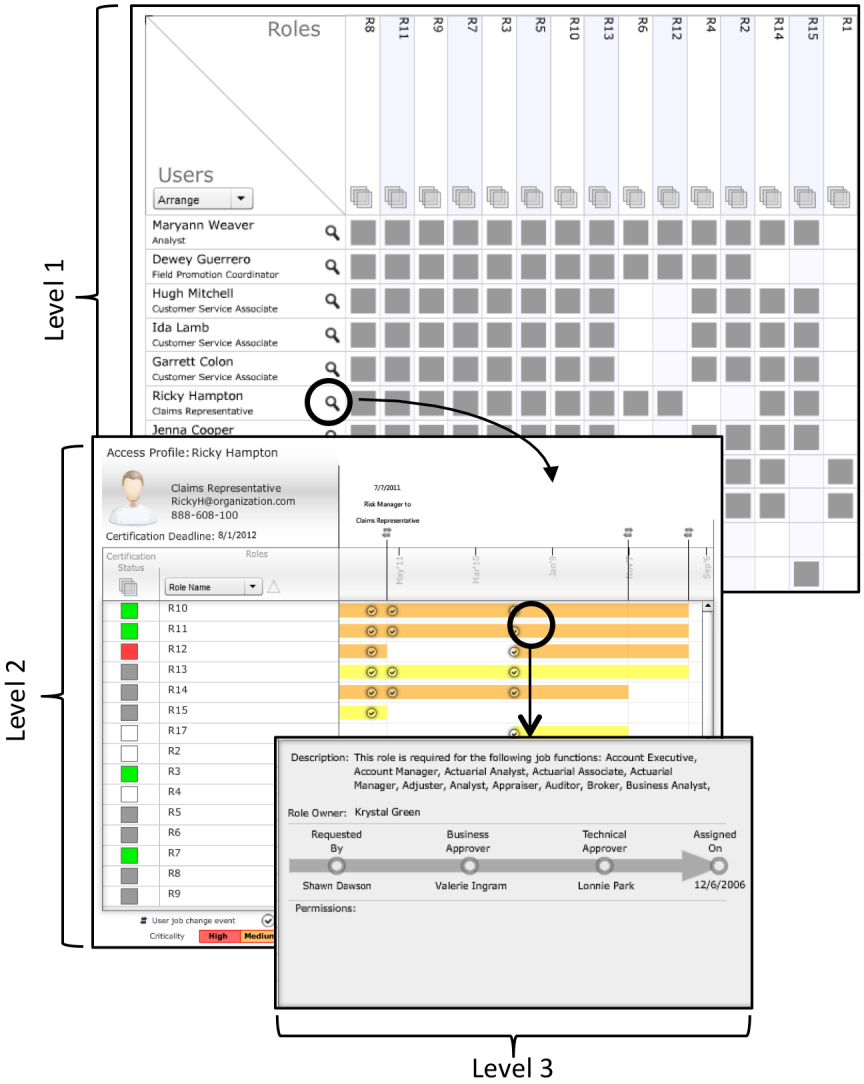
Omnigraffle

Balsamiq mockups


MS Visio

Adobe Flash

# Final Prototype



# Interface Demo

- http://goo.gl/qZTPF

# Future Plan: Lab study

- Lab study with three conditions: Proposed, CA Identity Manager, Aveksa
- Four tasks
  - Basic certification of known access-rights
  - Recurrent certification of known access-rights
  - Certification of  unknown access-rights
  - Risk assessment
- Compare interfaces in terms of:
  - Accuracy
  - Efficiency
  - Awareness

# Summary

- IT security management is challenging
- Conducting usability studies of ITSM tools is hard
- We presented different methods of addressing usability of ITSM tools:
  - Heuristic evaluation
  - Field study
  - Lab studies

# Questions ?

- *For more info:*

  *pooya@ece.ubc.ca (Pooya)*

  *rhootan@ece.ubc.ca (Hootan)*

  *beznosov@ece.ubc.ca (Kosta)*