# IdP - Best Current Practices
# Status Update

AAI Operations Committee, 16. September 2009, Berne

Halm Reusser
halm.reusser@switch.ch

Berne, 16. September 2009
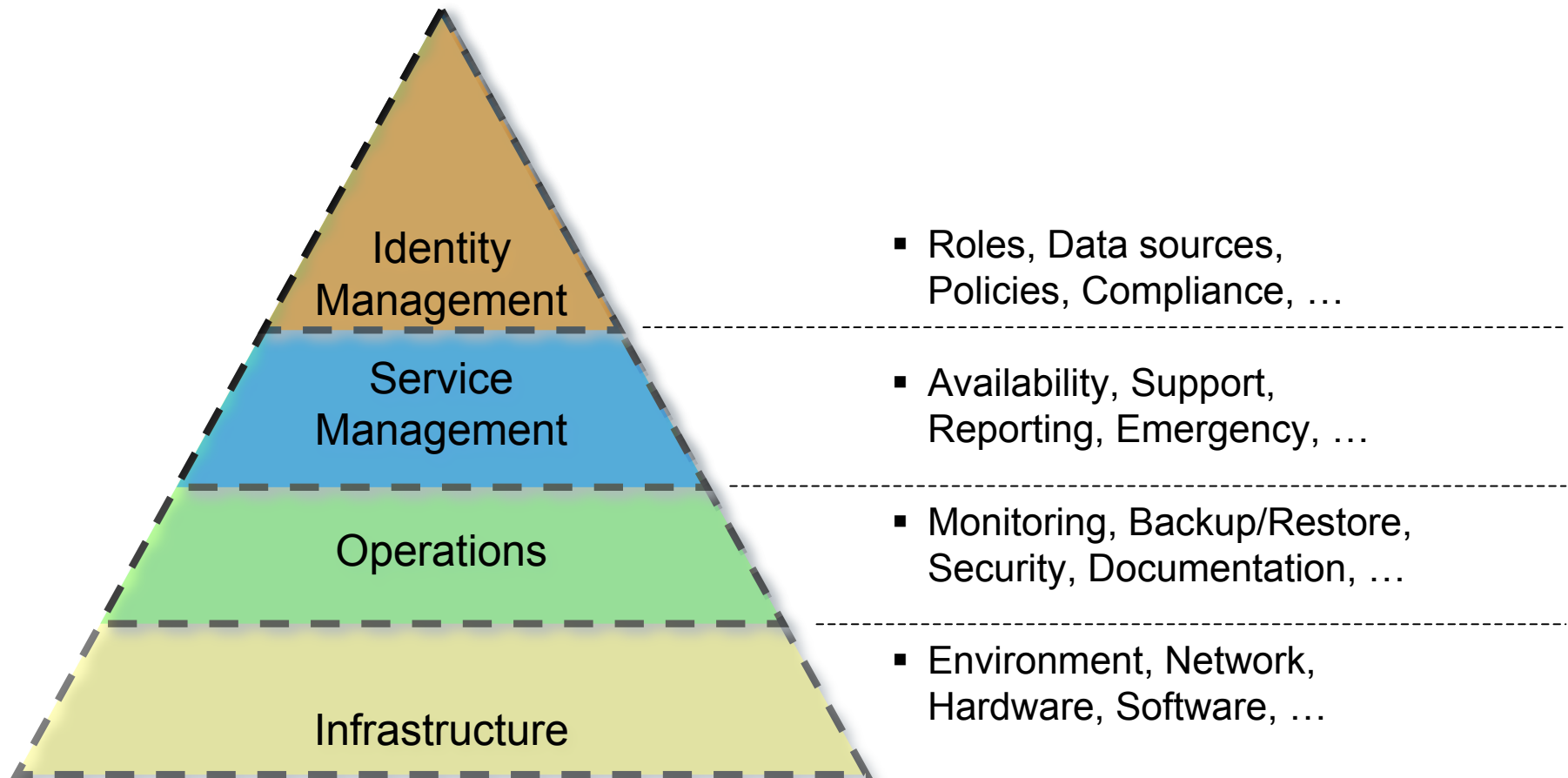
# Idea & Motivation

- AAI Service Agreement and AAI Policy form the ground rules for the federation.
  - AAI Policy uses rather vague and general terms.

- Need for more substantial requirements and recommendations, also for better guidance

- Collected best current practices for operating an Identity Provider in SWITCHaai.

- Basis for a future check list for *self audits* specifying *a service level for IdPs*

- As a next step: Same for the Service Provider there are a lot of common requirements and recommendations

# Benefit

- For Identity Providers, it

  specifies a guideline for how to operate the Identity Management service.

- For Service Providers, it

  discloses, what they can expect from Identity Providers.

- For end users, it

  increases the quality of their accounts, and therefore its value.

# Document structure & content

Requirements & recommendations about:



- Roles, Data sources, Policies, Compliance, …

- Availability, Support, Reporting, Emergency, …

- Monitoring, Backup/Restore, Security, Documentation, …

- Environment, Network, Hardware, Software, …

Pyramid levels (top to bottom):
- Identity Management
- Service Management
- Operations
- Infrastructure

# Current draft document, version 0.9

**PDF version**
- Usable for print out

**HTML version**
- Usable as reference

http://www.switch.ch/aai/bcp/

# Timeline

- Document development by SWITCH
- Status updates at former AAI OpCom meetings

**2. Sept.** ◆ Distributed version 0.8 to voluntary reviewers

- Review of version 0.8 by
    - Alexandre Roy & Etienne Dysli (University of Lausanne)
    - Roberto Mazzoni & Luzian Scherrer (University of Zurich)
    - Michael Hausherr (FHNW)

**16. Sept.** ◆ AAI OpCom meeting: Presentation version 0.9

- Review of version 0.9 by the SWITCHaai community

    Take your chance !

**22. Oct.** ◆ Deadline: Feedback to version 0.9

**29. Oct.** ◆ Final review by SWITCH

**5. Nov.** ◆ Publication Version 1.0

- Possible change requests for BCP Identity Provider
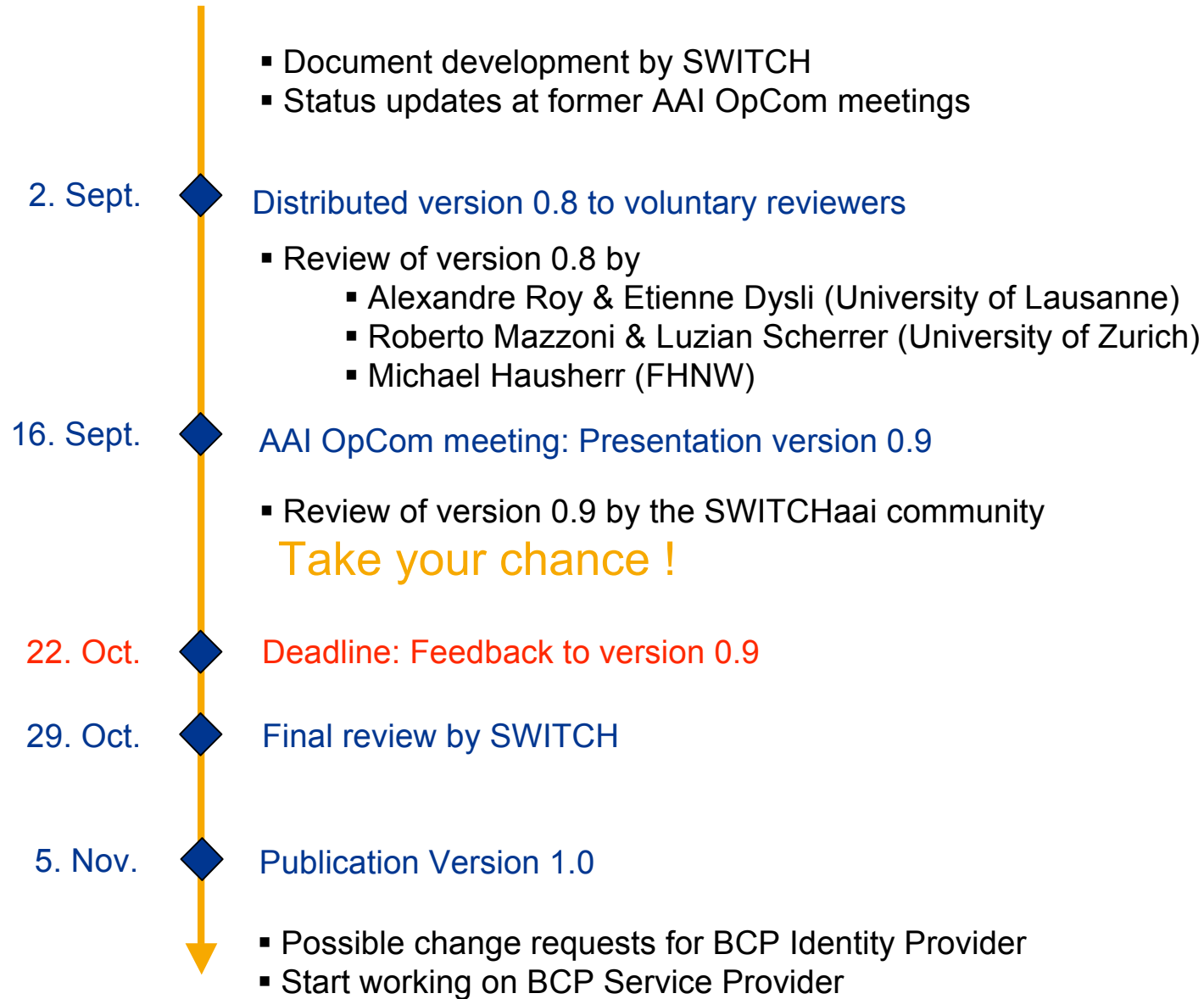- Start working on BCP Service Provider

# Feedback from voluntary reviewers (1)

- Michael Hausherr (FHNW)
  - The BCP are valuable and useful, they are written clearly and provide good guidance
  - The requirements and recommendations make sense and are to the point
  - For the final version I would like to have some of the requirements/recommendations supported with more background information (e.g. legal or contractual basis)

- Alexandre Roy & Etienne Dysli (University of Lausanne)
  - Good list of recommendations.
  - It contains many generals general items; IDM, AAI and Shibboleth specific issues are not highlighted enough.
  - It is difficult to apply all recommendations, because the person in charge of the IdP has not the possibility to change some processes or practices.

# Feedback from voluntary reviewers (2)

- Roberto Mazzoni & Luzian Scherrer (University of Zurich)
    - I think the document contains all the important things that one has to consider regarding the installation and operation of a SWITCHaai IdP. I'm also glad that the University of Zurich is compliant with pretty much all of the REQuirements und most of the RECommendations. Although some parts of the document seem a little too detailed to me and I think those could be formulated more generally with appealing to common sense.

# Your feedback is highly appreciated

- Download the HTML or PDF document from our website

- Take attention to the following points:
  - Are the important operational processes covered?
  - Are the relevant requirements and recommendations described?
  - Are there requirements, which should be recommendations (too hard)
  - Are there recommendations, which should be requirements (too soft)

- Review can done, either by:
  - Mail or telephone feedback
  - PDF comments
  - Microsoft Word revision control (RTF document)
  - Hand notes (scanned)

http://www.switch.ch/aai/bcp/    Deadline: 22.10.2009