Migrating to OSPP

How we switched an ongoing evaluation to a new PP

Diana Robinson, IBM
Gerald Krummeck, atsec information security
William Penny, IBM

11th Annual ICCC
September 22, 2010
Anatalya, Turkey

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Other company, product, or service names may be trademarks or service marks of others.

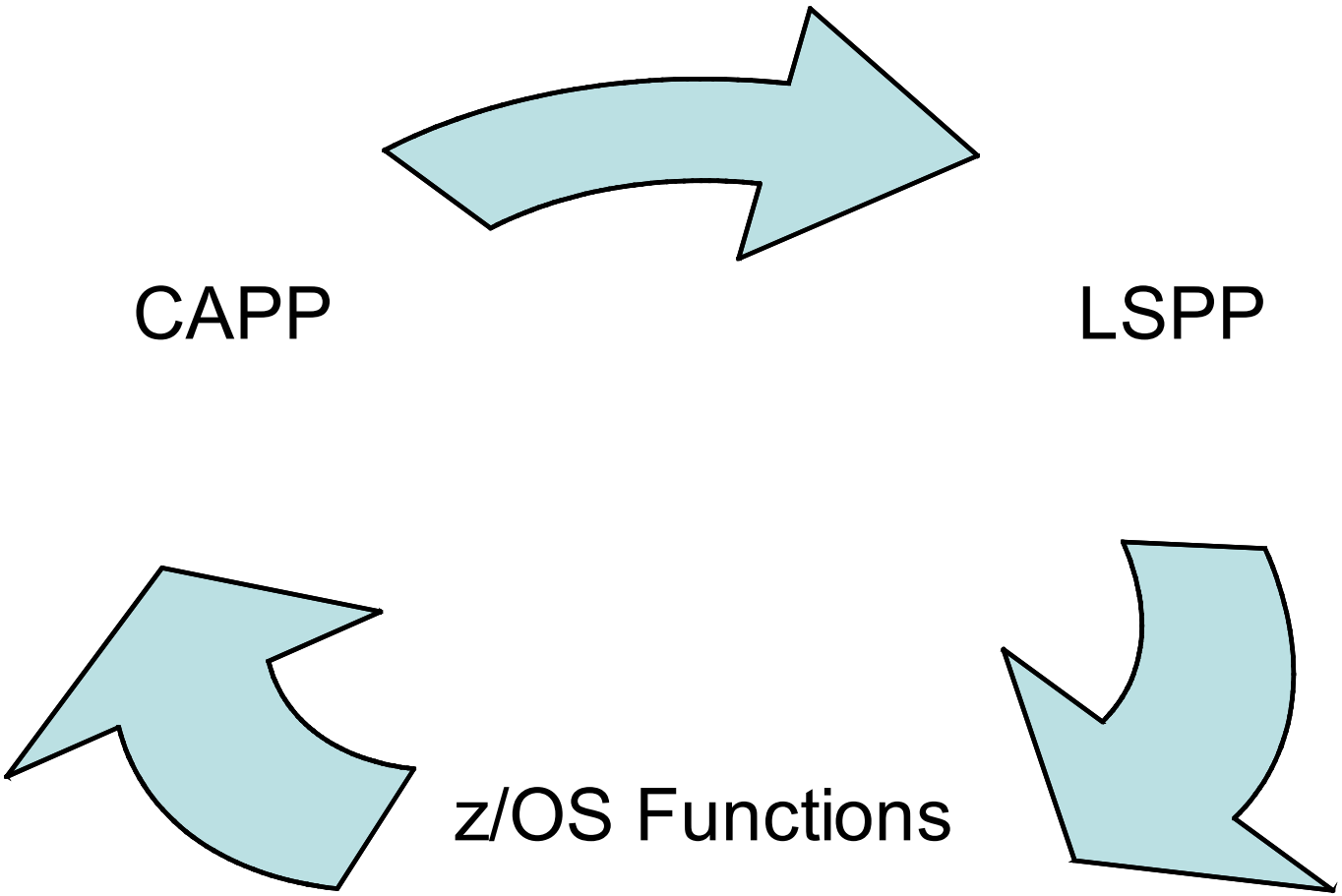
© IBM corp, atsec information security

OSPP

- "With the EAL4 Common Criteria certification of z/OS V1R11, IBM was the first exploiter of the newest addition to the list of Common Criteria Protection Profiles, the Operating System Protection Profile (OSPP). This presentation will provide insight into the experiences of the Evaluator (Atsec) and Vendor (IBM) during the birth of the OSPP concept, the development of the standards, and the final implementation."

© IBM corp, atsec information security

Security Target

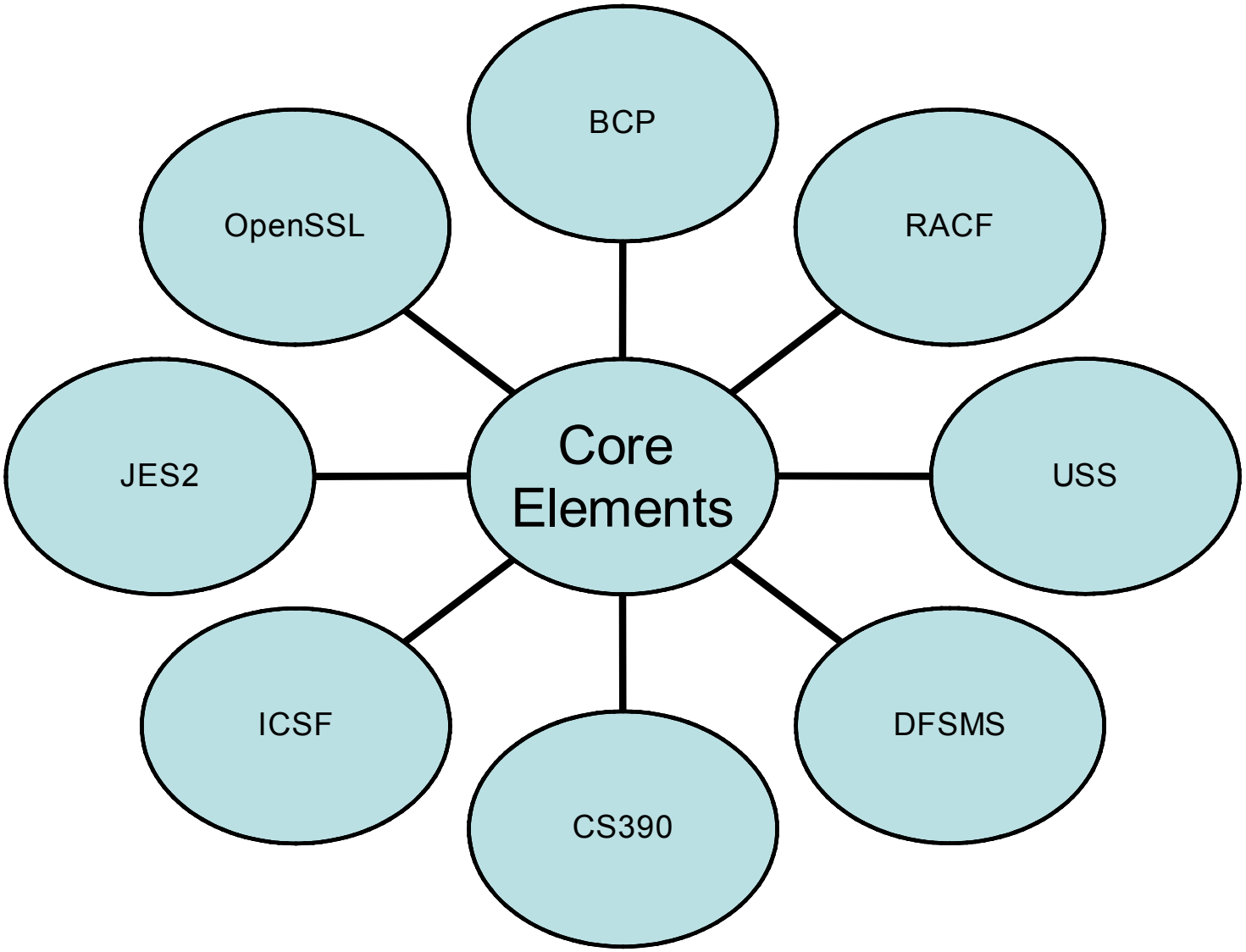


© IBM corp, atsec information security

Initial Strategy

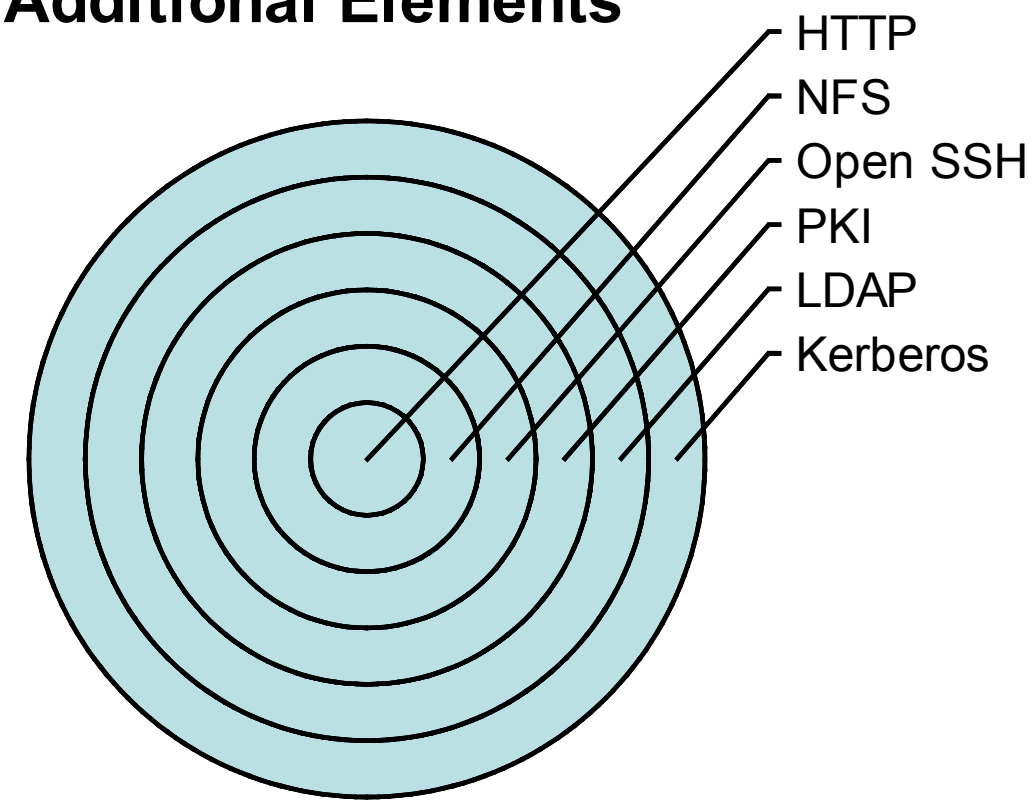
- Switch to OSPP was risky near end of evaluation work
- Minimize risk:
  - No new functions
    - Restrict changes to ST and mappings from ST to other documentation
  - Claim only extended packages which are fully covered by already evaluated functionality
  - Using XML tools to rewrite ST will help to ensure consistency
- Extended packages:
  - Labeled Security
  - Advanced I & A

© IBM corp, atsec information security

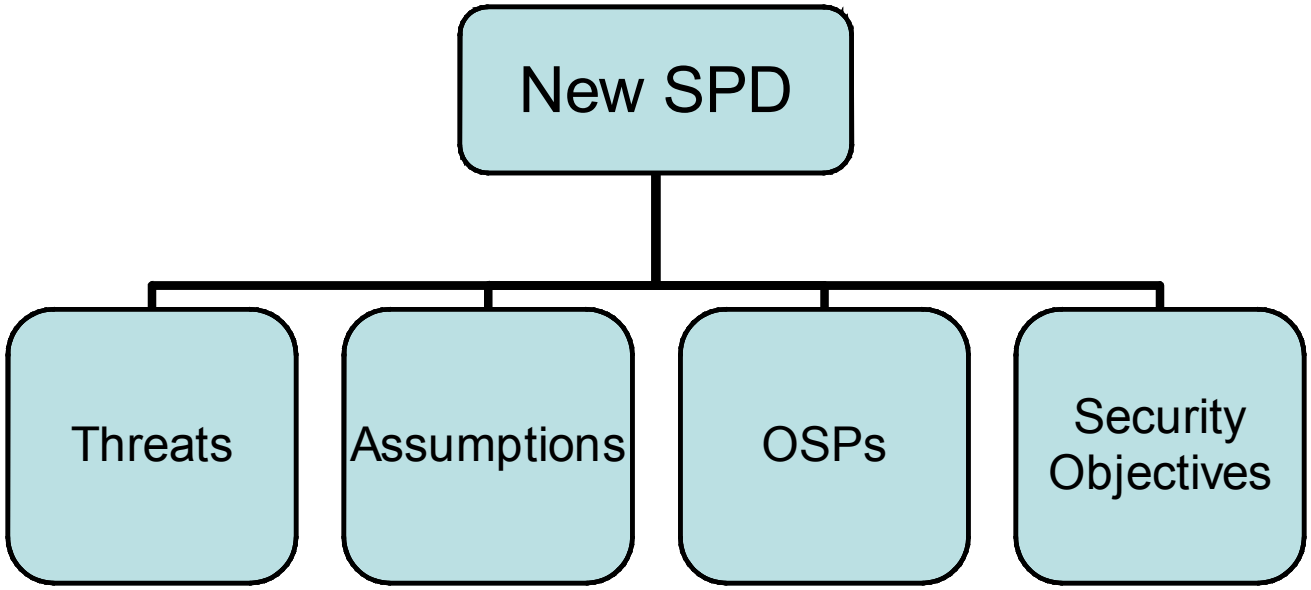


© IBM corp, atsec information security

Additional Elements



© IBM corp, atsec information security

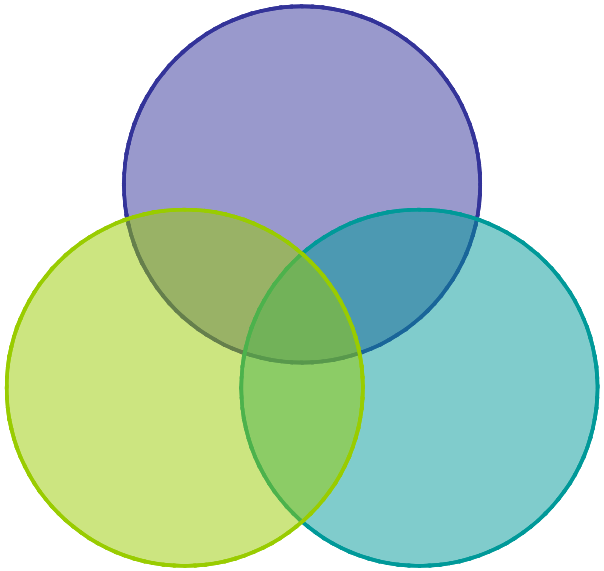


Strategy: Use SPD from OSPP, replacing LSPP/CAPP SPD

© IBM corp, atsec information security

New ST

New SFRs

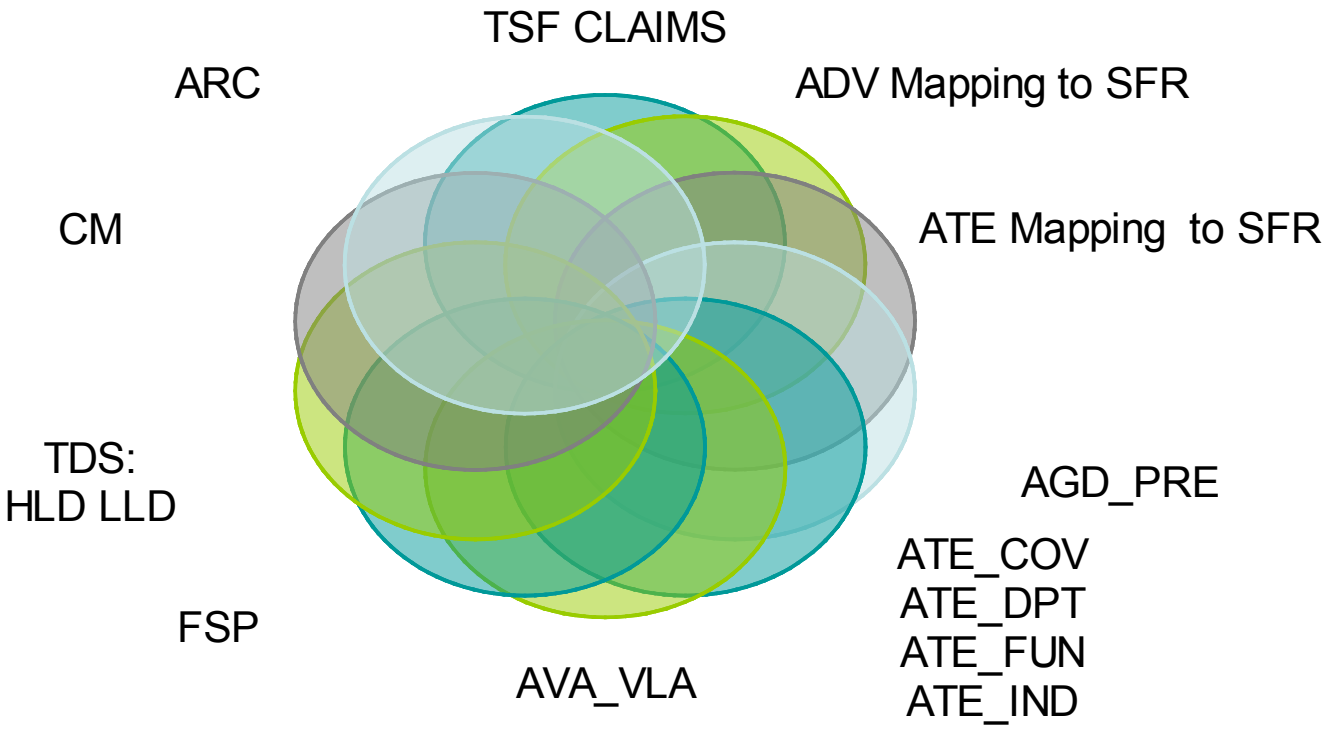


New
TSF to SFR
Mapping

Updated
Rationale

© IBM corp, atsec information security

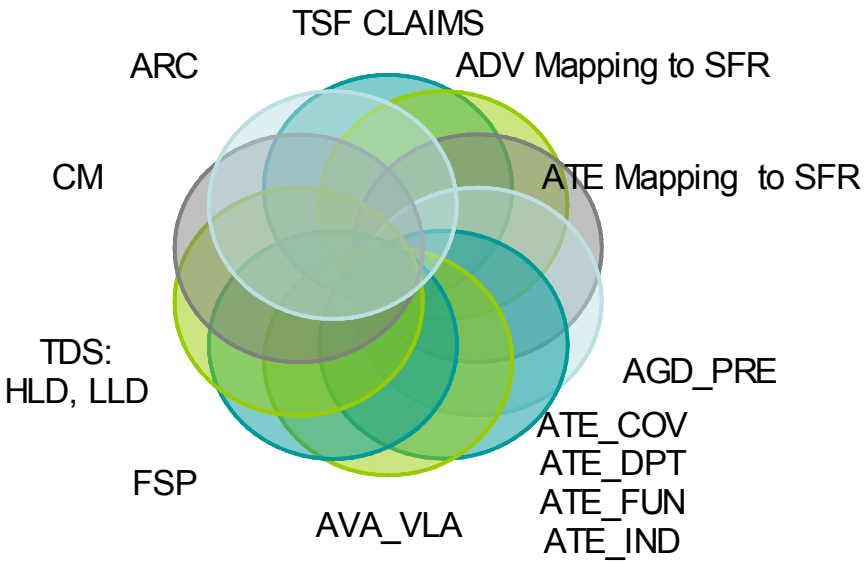
What remained the same?



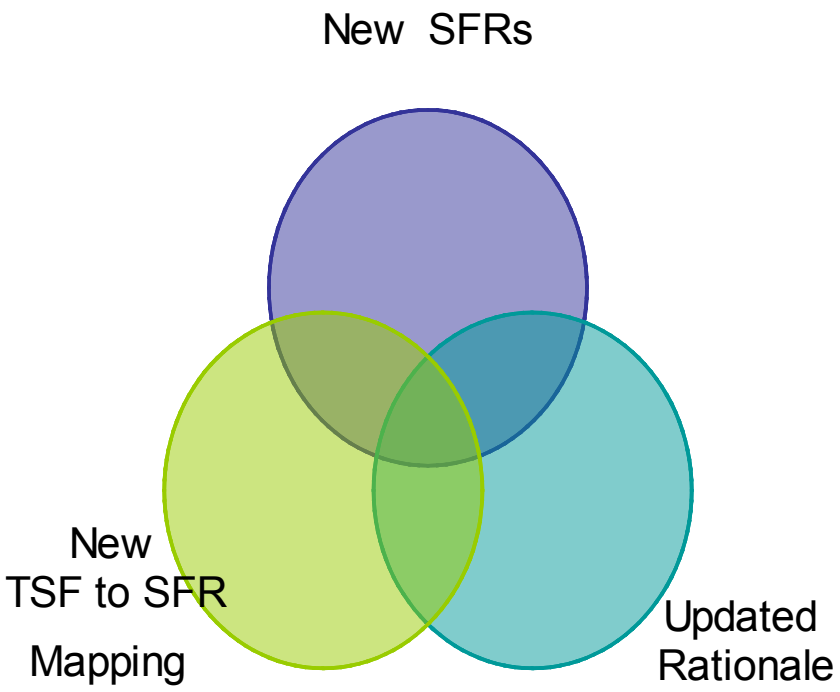
© IBM corp, atsec information security

COMPARISON of ST Changes

Remained the Same



Changed



© IBM corp, atsec information security

Unplanned and Unexpected SFRs

- FCS_RNG (used BSI Test Suite)
- FTA_SSL
  - Irrelevant: No “direct” sessions
  - Current CC cannot deal with conditional SFRs
- FDP_IPC (packet filters)
  - So far, only RACF’s access control to the firewall functions had been claimed
  - Additional Design work (TDS)
  - Required additional unexpected testing
    - Testcases already existed
  - Test documentation updated

© IBM corp, atsec information security

Summary: Evaluator Experience

- Migration was smooth, even though evaluation was in advanced stage
- Major effort: re-writing ST and ASE report
- Numbered Security Claims in TDS helpful to minimize changes
  - No changes in mappings required for TSF and TSFI (FSP, TDS, ATE)
- Few changes for additional functions resulted in few additional changes to evaluation reports
- Tool-based ST authoring reduced ASE work
- **OSPP proven to work for complex system**

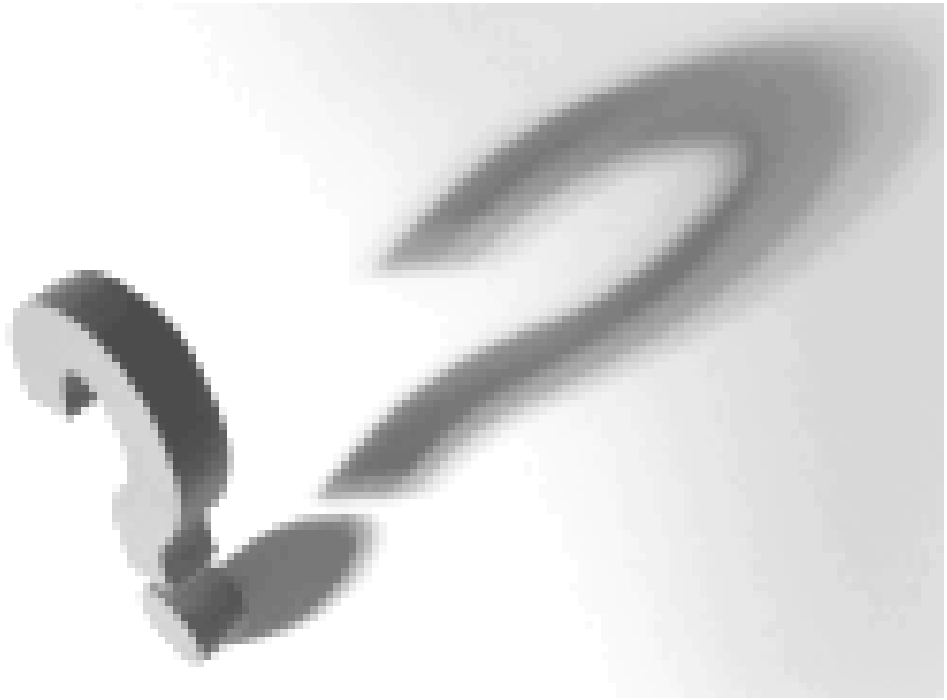
© IBM corp, atsec information security

Summary: Vendor Experience

- OSPP Migration was made easier by working closely with evaluator and certifier.
- New SFRs caused some rework during end of cycle.
- Extended evaluation schedule – for good results.

© IBM corp, atsec information security

Questions



© IBM corp, atsec information security

Contact

- Diana Robinson, IBM Corporation
  - 2455 South Road
    Poughkeepsie NY, 12603
    dianar@us.ibm.com
    (845) 435-4865

- William Penny, IBM Corporation
  - 2455 South Road
    Poughkeepsie NY, 12603
    wpenny@us.ibm.com
    (845) 435-3010

- Gerald Krummeck, Atsec Information Security, GmBH
  - Steinstrasse 70
    81667 Munich Germany
    Gerald.Krummeck@atsec.com
    89-442-49852

© IBM corp, atsec information security