RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: GRM-R01

Compliance Goal: Implementing Segregation Of Duties In An Organization

Lenka Fibikova

Independent Consultant

Why Segregation of Duties

- Compliance with the national laws requiring correctness of the financial information and financial reporting
- Business requirements on integrity of business information

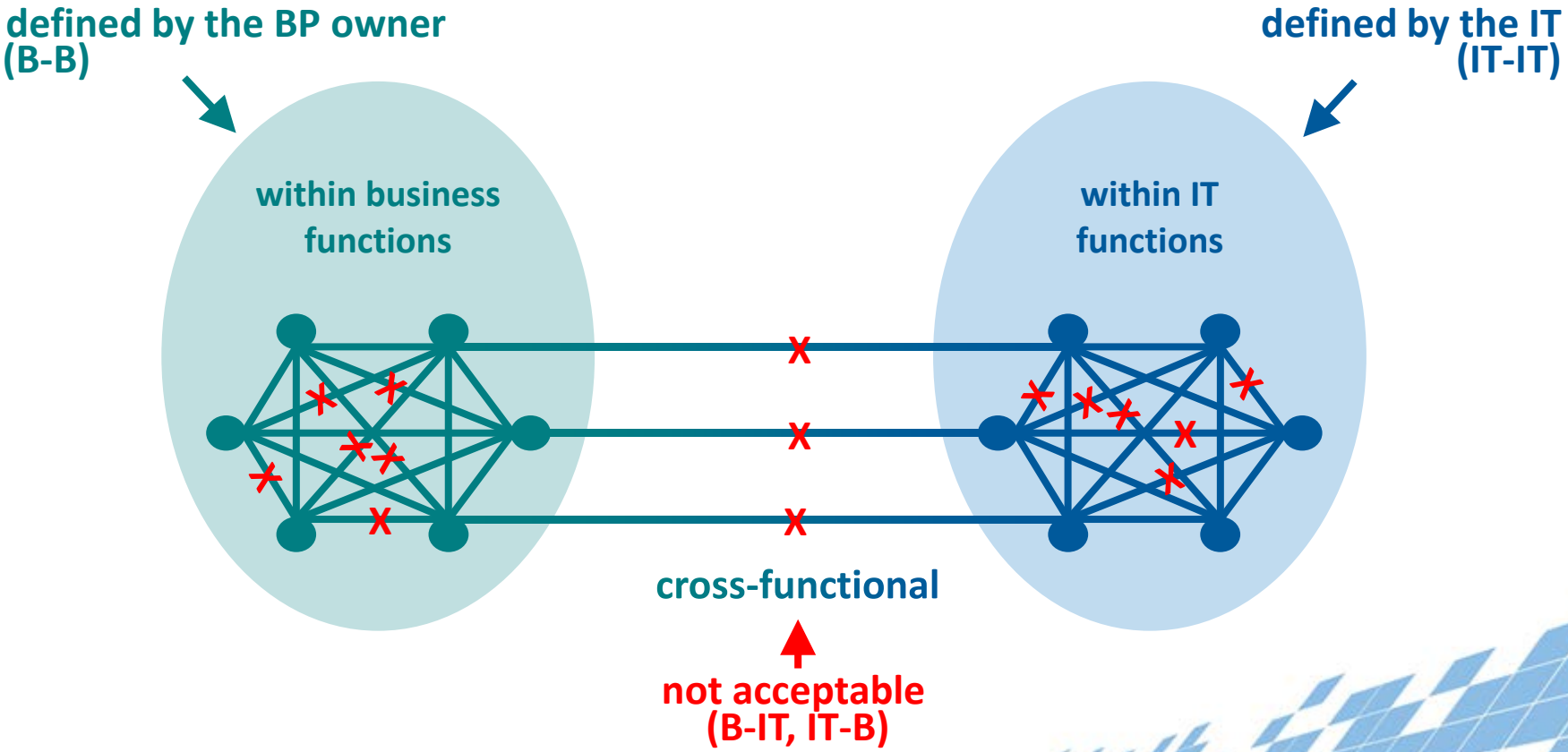
The story starts with…

- Identified misuse
- Findings from an external auditor
- Findings from an internal auditor
- Push from an enlightened leader

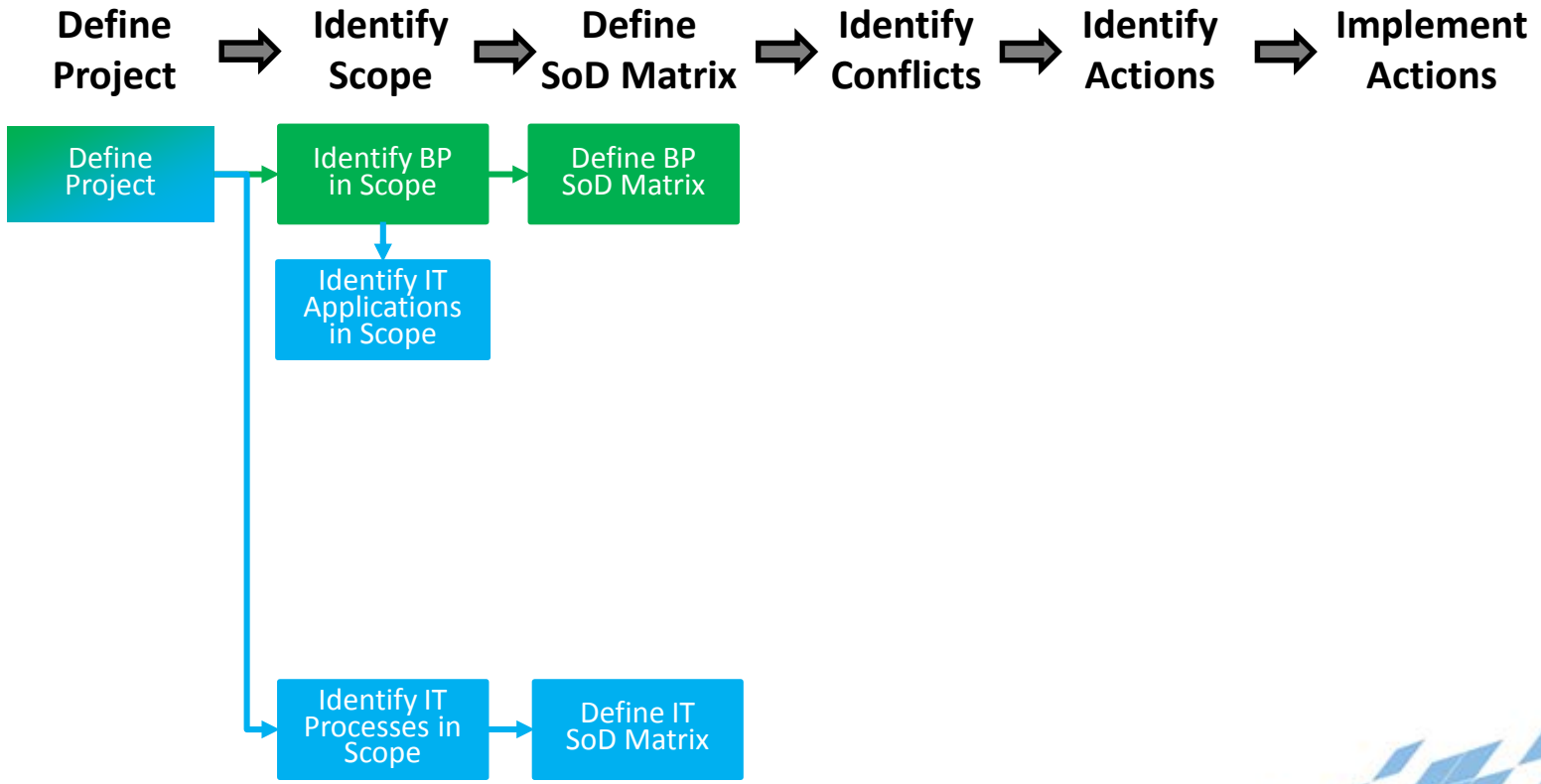
Challenges

- **Challenge 1:** To make Business Process Owners responsible for segregating business functions (e.g., transactions, invoicing)
- **Challenge 2:** To convince IT management that uncontrolled access of IT users to the business data is a bad idea
- **Challenge 3:** To take the toy out of the Business Process Owners' hands (shadow IT)
- **Challenge 4:** To make it clear that IT functions (e.g., access control) are no exception from segregation of duties

Areas of concern



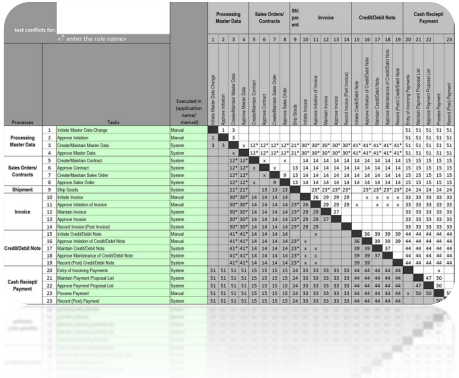
Implementing SoD Step by Step



Exercise: Define a B-B SoD Matrix

1. Document the process, its sub-processes and tasks
2. Identify SoD-relevant tasks ◄
3. Create the SoD matrix

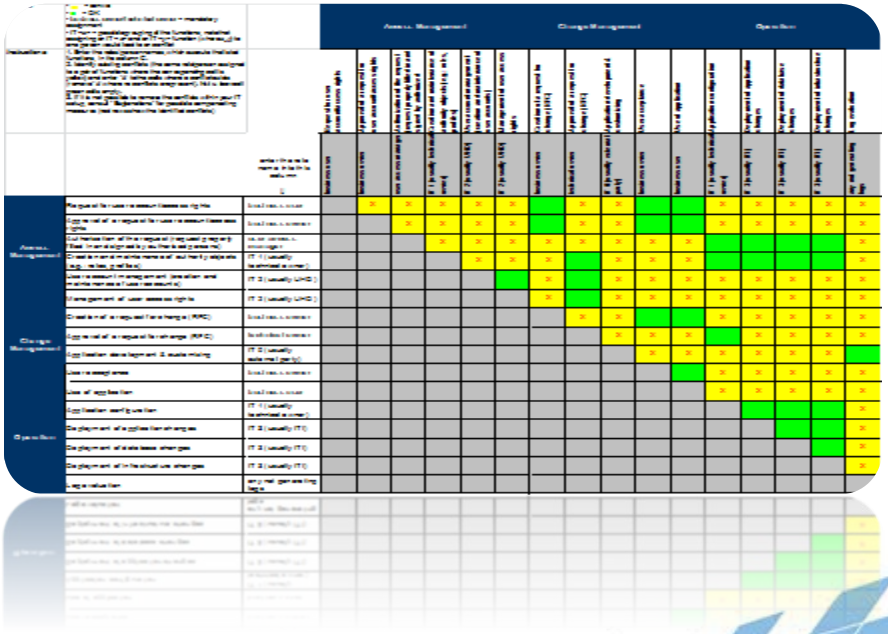
Processes		Tasks	Executed in (application name/ manual)
Process 1	1	Task 1.1	application/manual
	2	Task 1.2	application/manual
	3	Task 1.3 ◄	application/manual
	4	Task 1.4 ◄	application/manual
	5	Task 1.5 ◄	application/manual
	6	Task 1.6	application/manual
	7	Task 1.7	application/manual
	8	Task 1.8 ◄	application/manual
	9	Task 1.9 ◄	application/manual
	10	Task 1.10	application/manual
	11	Task 1.11	application/manual
	12	Task 1.12 ◄	application/manual
	13	Task 1.13 ◄	application/manual
	14	Task 1.14	application/manual
Process 2	15	Task 2.1 ◄	application/manual
	16	Task 2.2 ◄	application/manual
	17	Task 2.3	application/manual
	18	Task 2.4	application/manual
	19	Task 2.5	application/manual
	20	Task 2.6 ◄	application/manual
	21	Task 2.7 ◄	application/manual
	22	Task 2.8	application/manual
	23	Task 2.9	application/manual



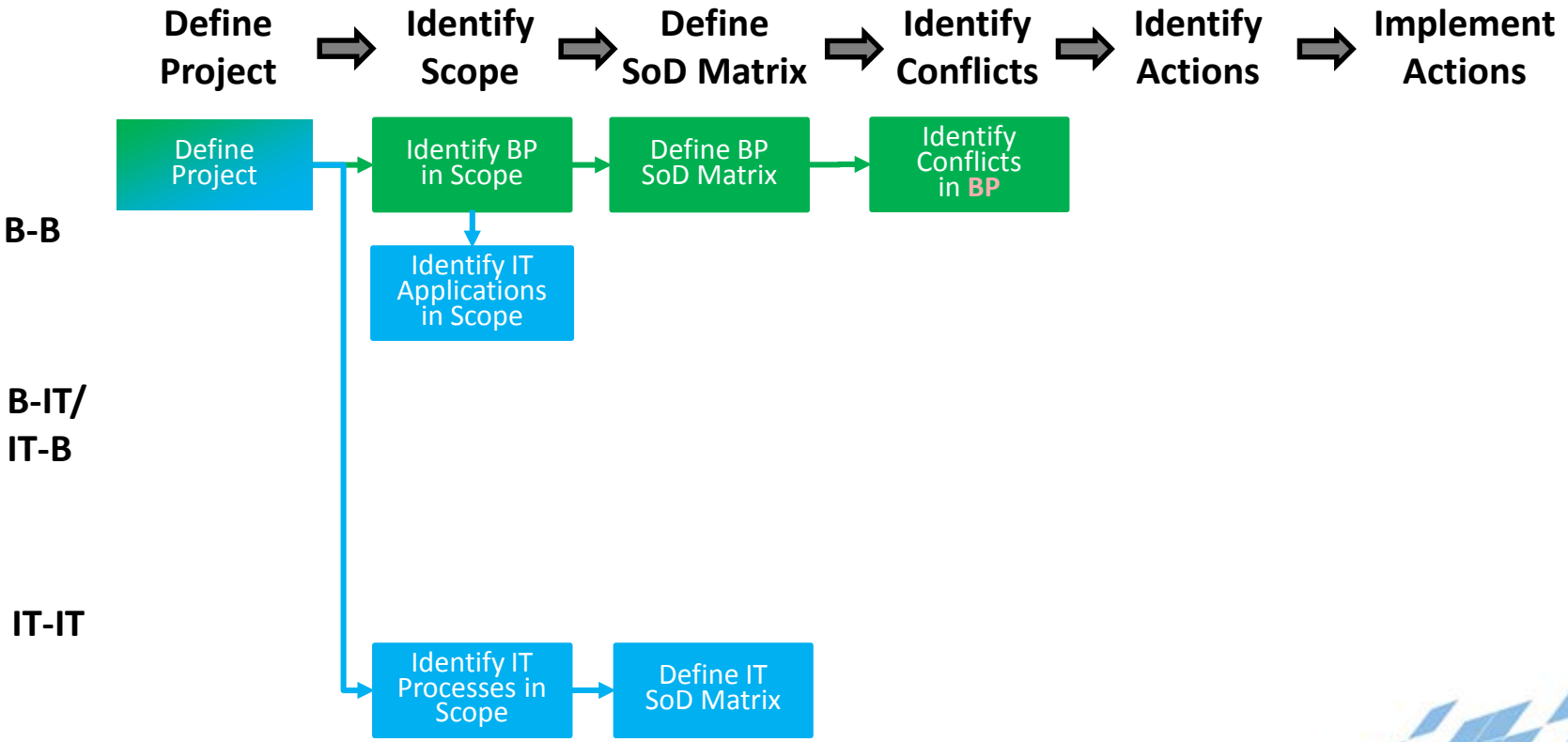
Exercise: Define an IT SoD Matrix

Areas of responsibility:

- Change Management
- Access Management
- Operation

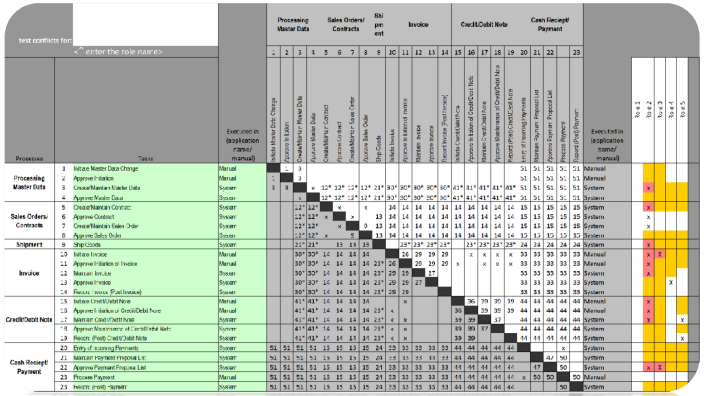


Implementing SoD Step by Step

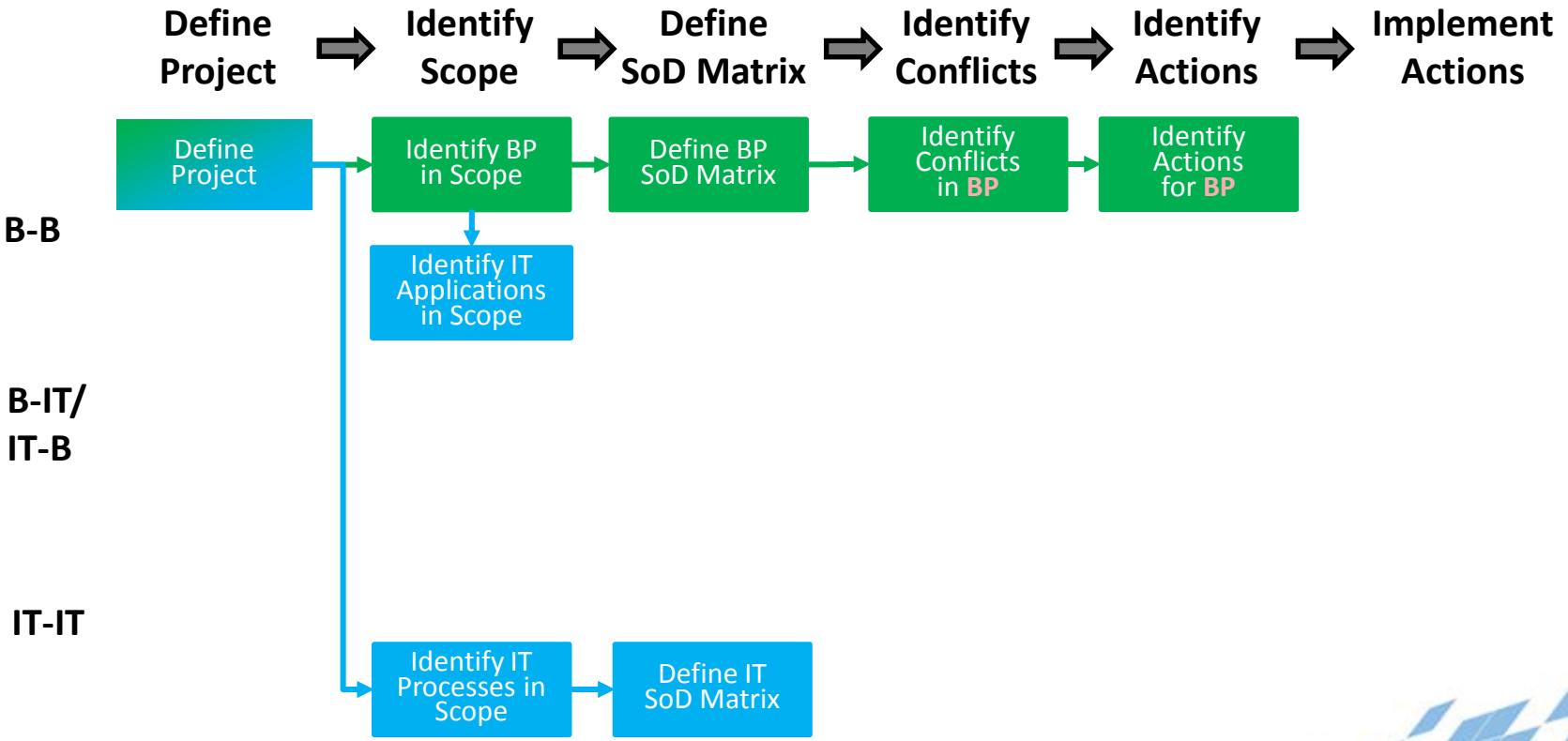


Exercise: Identify conflicts

1. Identify business roles
2. Document which SoD-relevant tasks each of the roles executes
3. Verify whether any of the roles currently violates defined SoD rules



Implementing SoD Step by Step

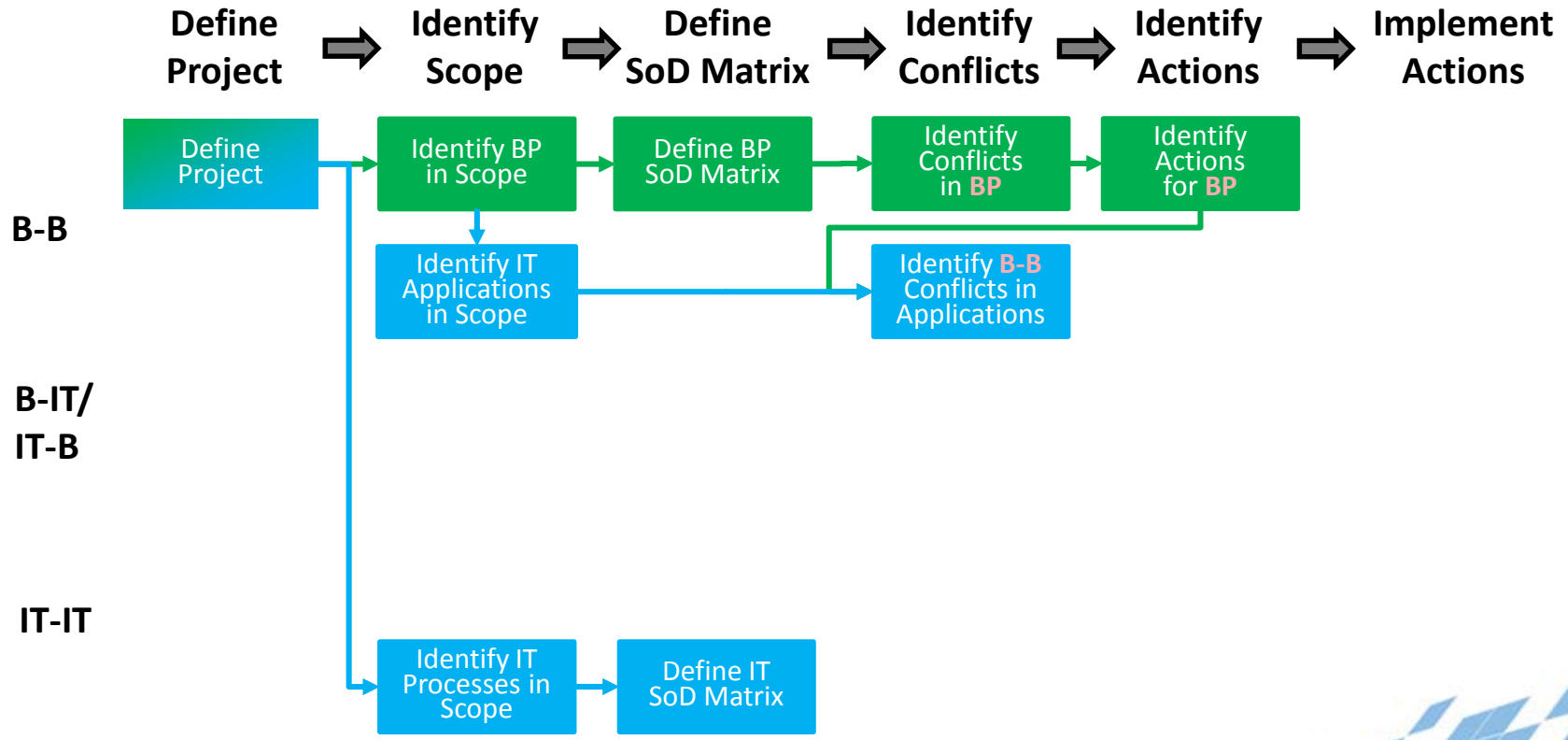


Exercise: Identify Actions

For each of the identified conflicts, an action **has** to be defined and documented:

- Immediate **removal of the conflict**
- Immediate **setup of administrative measures** to minimize the risk
- **Implementation plan** for removal of the conflict or for setup of administrative measures to minimize the risk
- **Formal risk acceptance** by the Business Process Owner (might not be possible for some risks)

Implementing SoD Step by Step

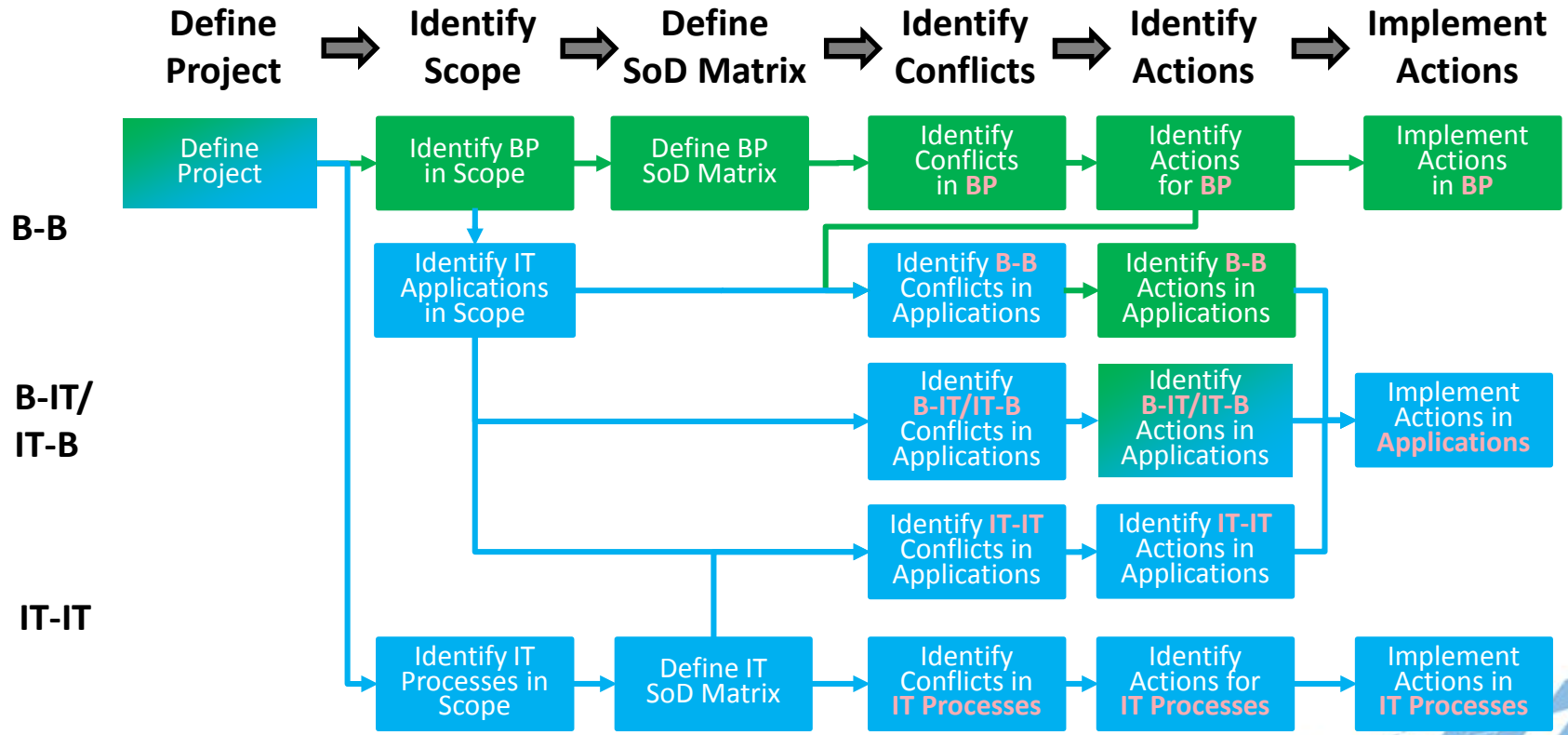


Exercise: Mapping the SoD Matrix to IT

1. Identify which applications and application functions support the tasks
2. Extract which user IDs use the identified functions
3. Identify SoD conflicts

Processes		Tasks	Executed in (application name/ manual)	Business Roles	Role 1	Role 2	Role 3	Role 4	Role 5	Role 6	Role 7	Functions supporting the task	Users	UID 1	UID 2	UID 3	UID 4
Process 1	3	Task 1.3	application/manual		x												
	4	Task 1.4	application/manual					x		x							
	5	Task 1.5	application/manual		x					x							
	8	Task 1.8	application/manual				x										
	9	Task 1.9	application/manual							x							
	12	Task 1.12	application/manual				x										
	13	Task 1.13	application/manual					x									
Process 2	15	Task 2.1	application/manual			x											
	16	Task 2.2	application/manual						x		x						
	20	Task 2.6	application/manual		x				x								
	21	Task 2.7	application/manual								x						

Implementing SoD Step by Step



Lessons Learned: Good Approach

1. Small, transparent, understandable steps
2. Documentation of processes where not yet done
3. Improvement of business processes
4. Segregation of duties for both manual and IT-supported tasks
5. Segregation of duties across applications
6. Compliance

Lessons Learned: The Hard Part

1. Be ready to deal with legacy applications
2. Compliance of shadow IT is expensive
3. When business units do not want to give up the access management functions
4. Sustainability or Consider a tool to keep the status clean

Apply in Your Organization

- **Next week** you should:
  - Verify how you handle integrity of your financial data and whether Segregation of Duties has been consistently applied
  - Consider whether there are any further (business-related) reasons for SoD
- **In the first three months** you should:
  - If there is no consistent approach for SoD, initiate a discussion with the senior management
- **Within six months** you should:
  - Set up an SoD project
  - Remember: Implementation of SoD takes longer than it might appear

Questions