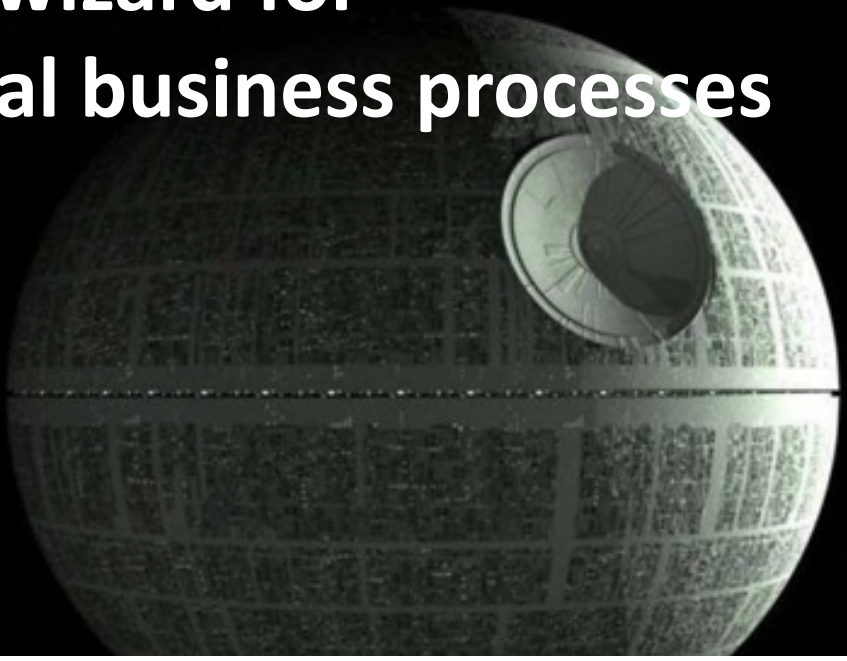
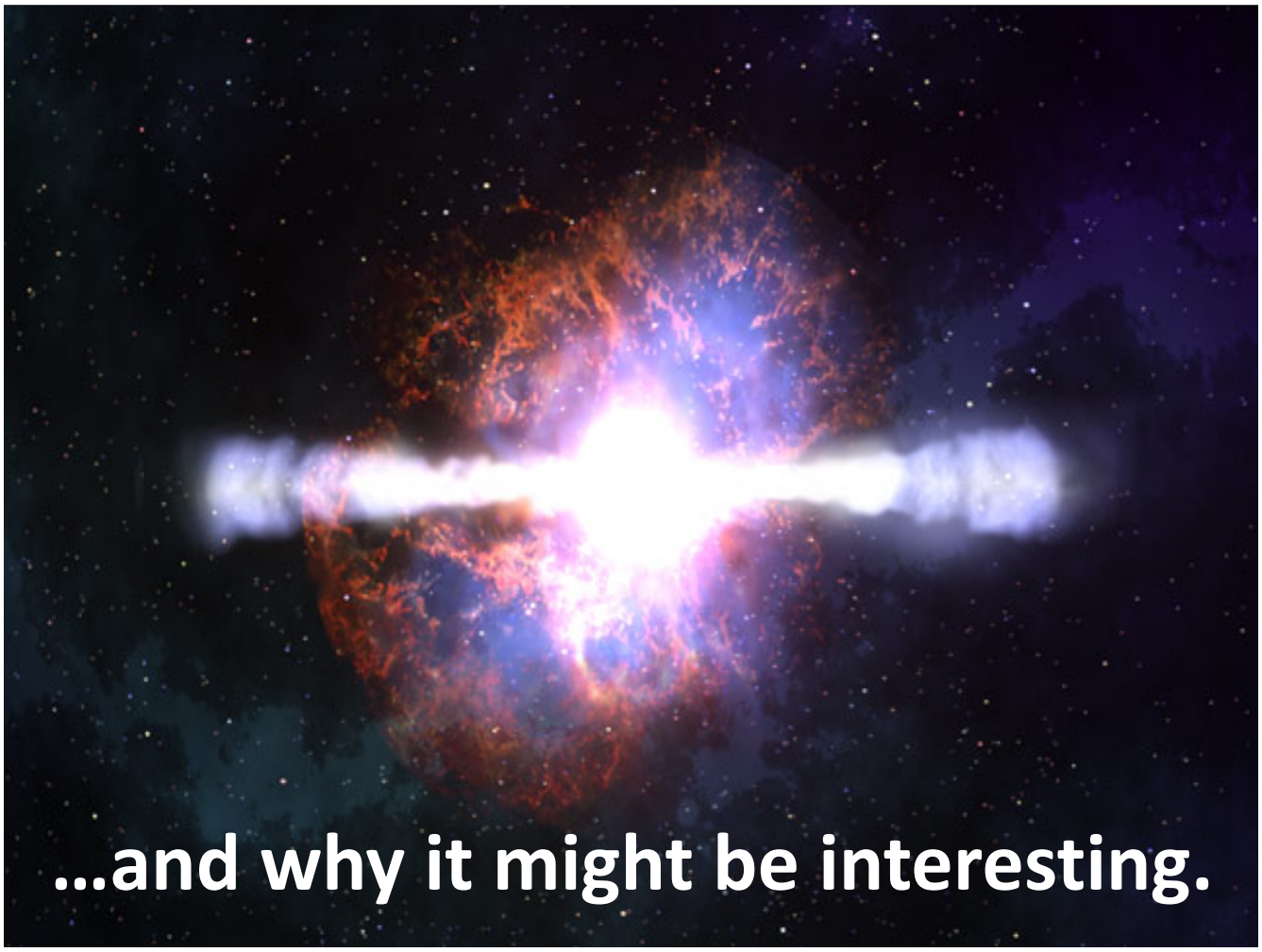
Modeling wizard for confidential business processes



Andreas Lehmann
Niels Lohmann

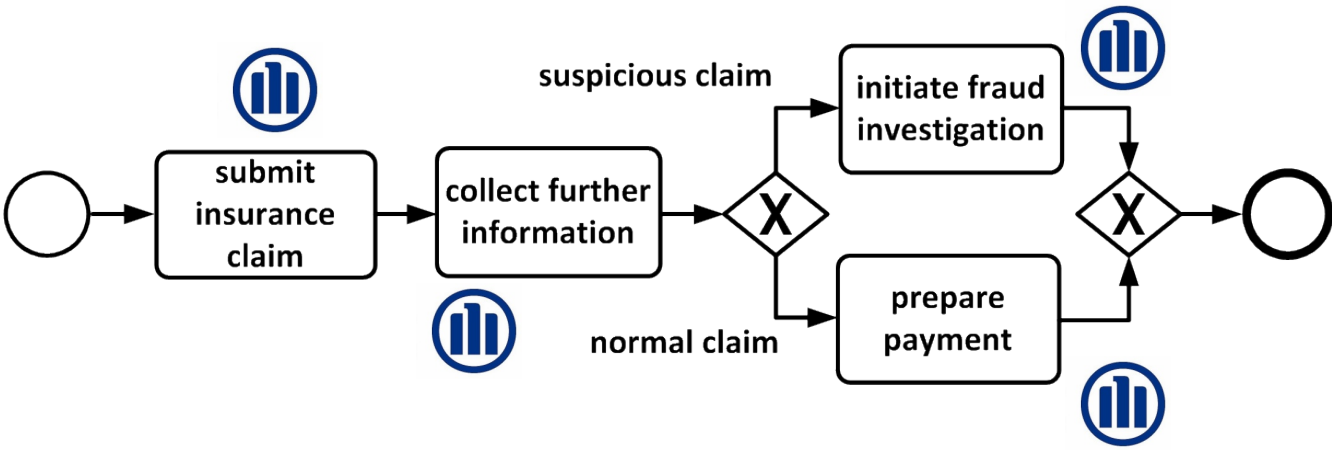
Universität Rostock
Traditio et Innovatio



…and why it might be interesting.

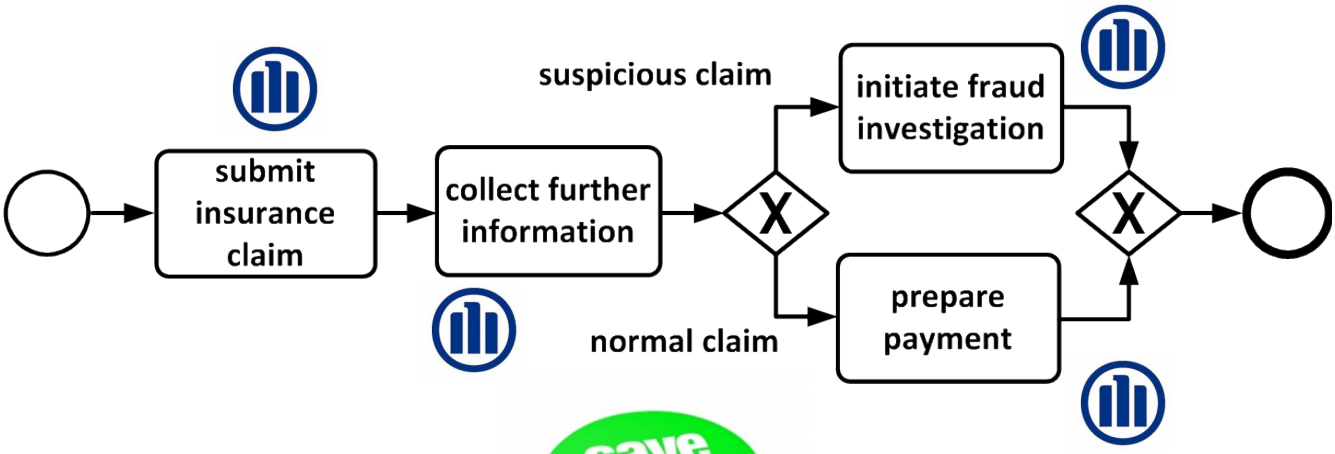
Our business process 1

Allianz

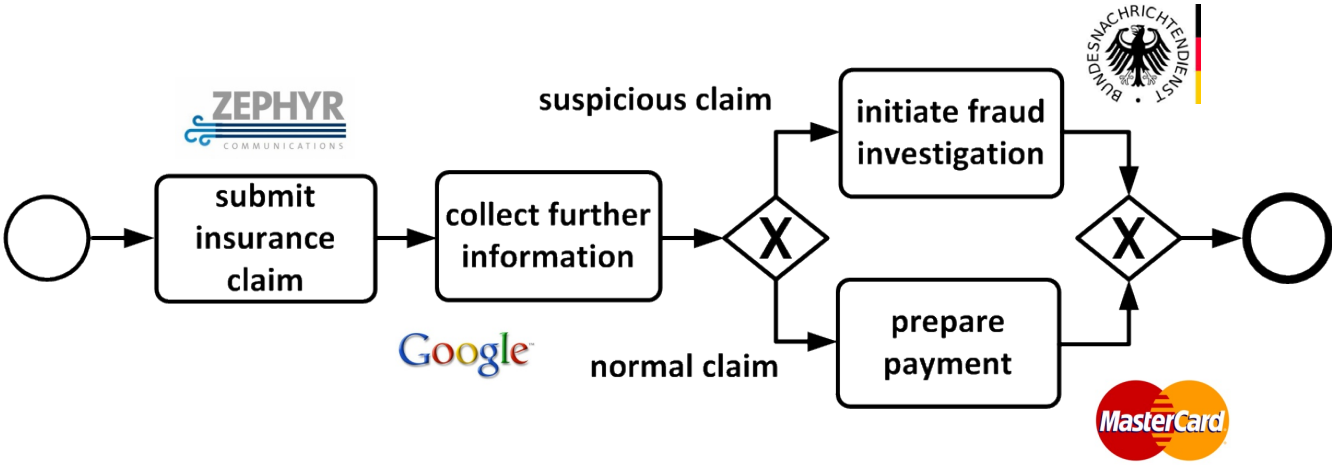


Our business process 2

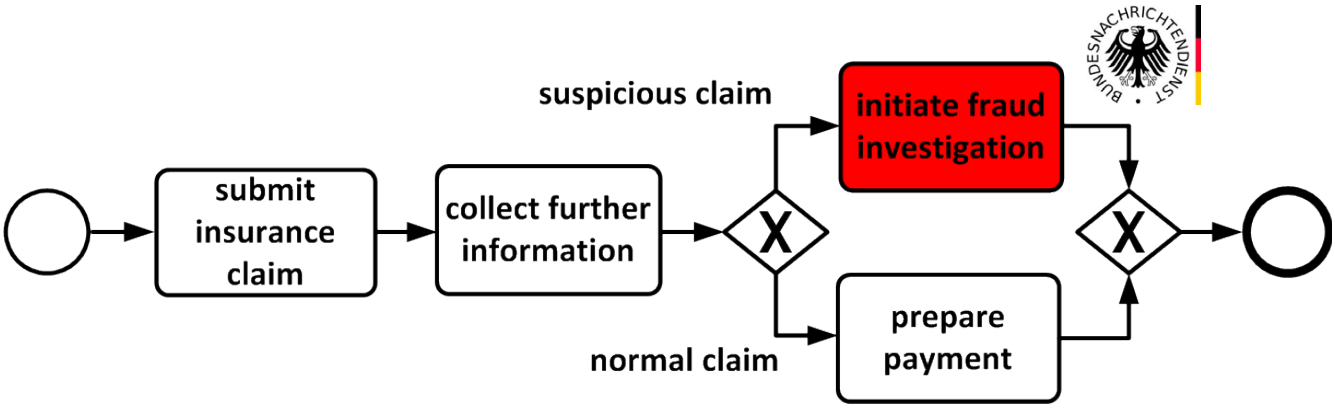
Allianz



Outsourcing tasks… 2

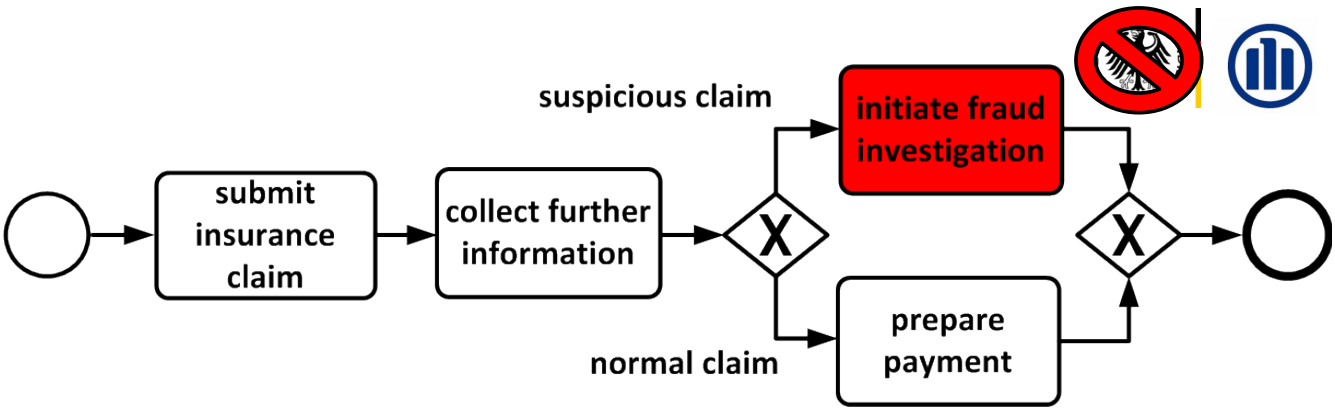


…considering confidentiality 3



Some tasks may be confidential.

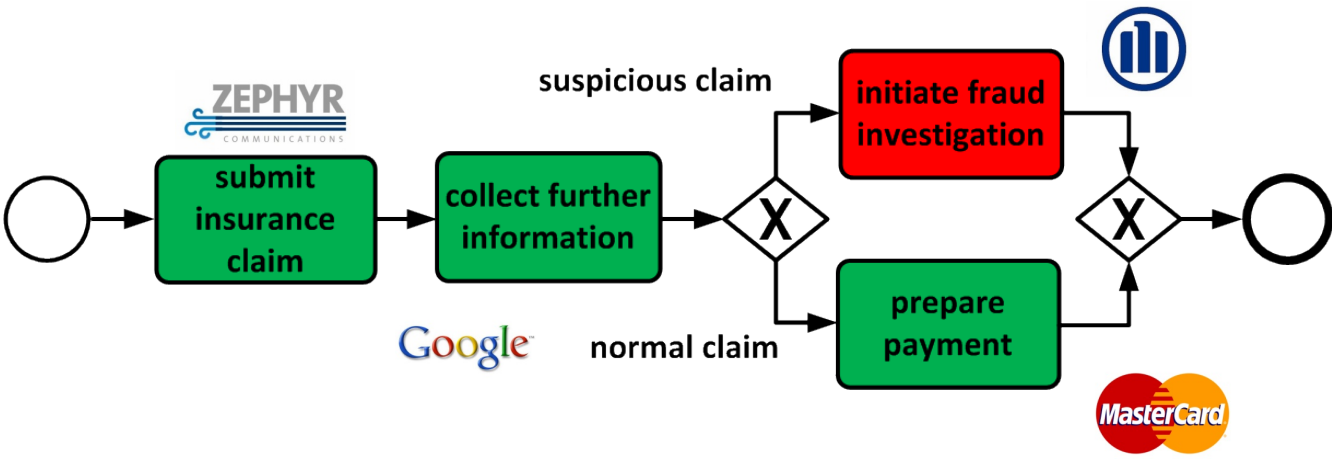
…considering confidentiality 3



Some tasks may be confidential.

Those tasks shall **remain inhouse**.

…considering confidentiality 3



Some tasks may be confidential.

Those tasks shall **remain inhouse**.

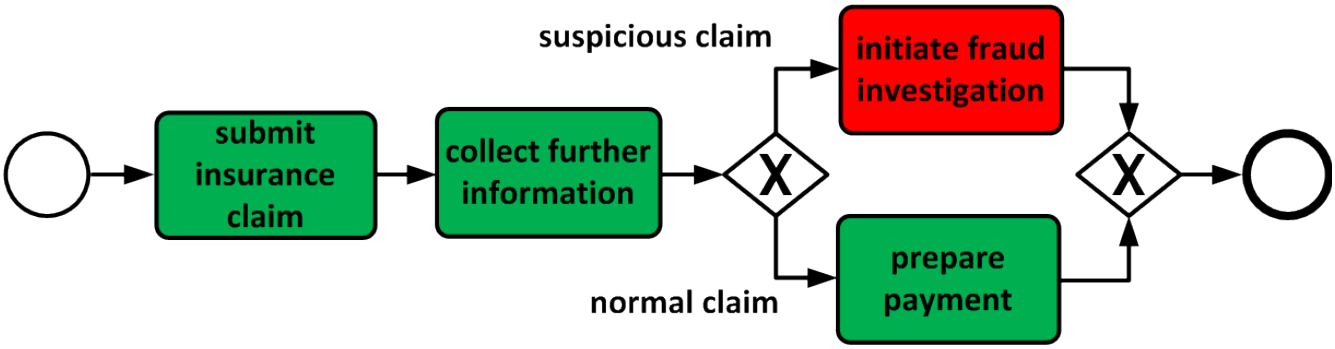
Others may be outsourced.

Confidentiality

What can be outsourced without revealing confidential tasks?

How to express confidentiality?

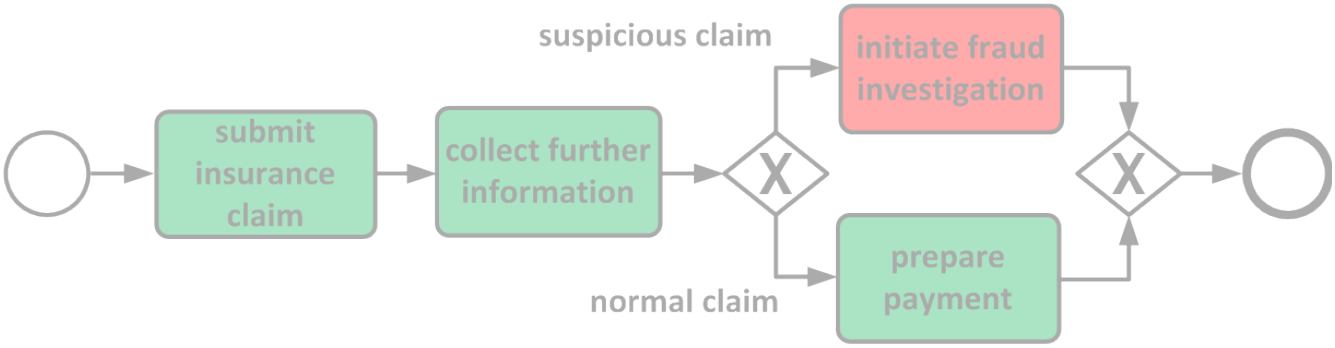
How to express confidentiality?



Assign the tasks.

Confidentiality 5

How to express confidentiality?



Assign the tasks.

How to check confidentiality?

Outsourced tasks may not learn anything about confidential tasks.

Non-Interference 6

Assumptions

Whole process is known and outsourced tasks are observable.

Non-Interference 6

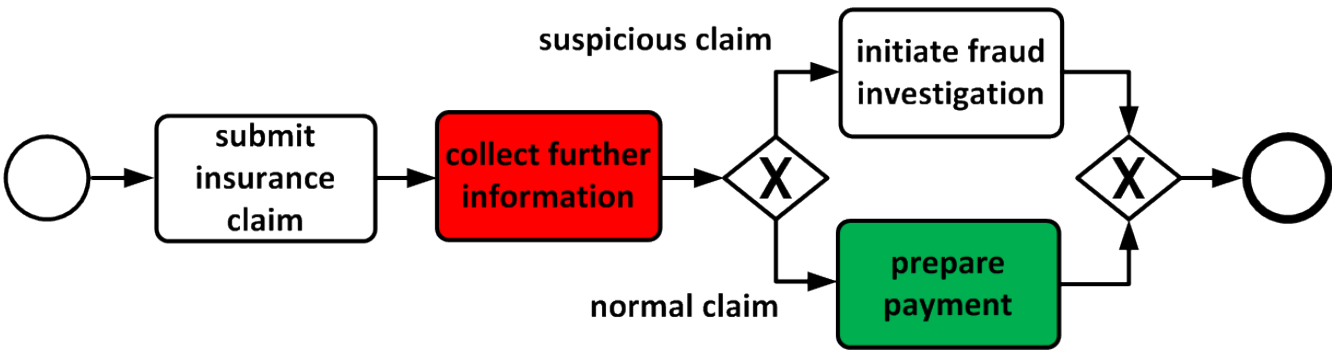
Assumptions

Whole process is known and outsourced tasks are observable.

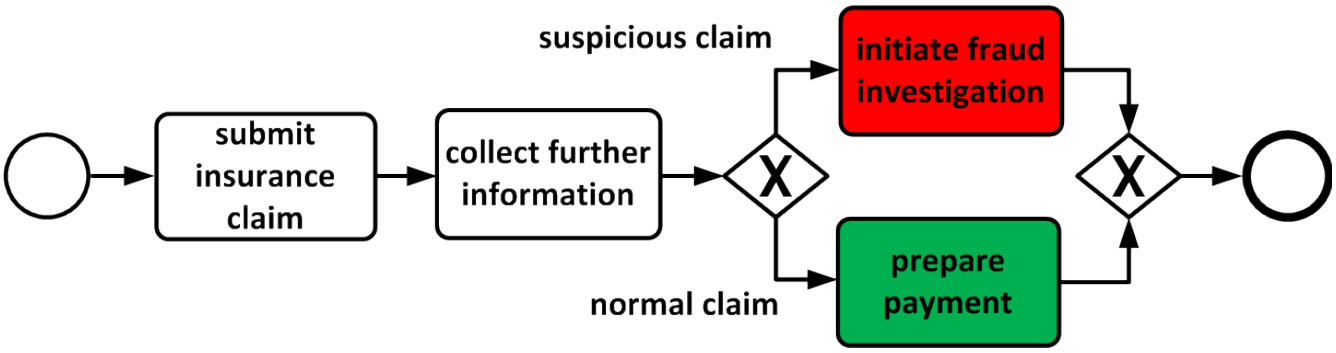
How to learn anything:

Possible Interference 7

Outsourced depends on confidential.



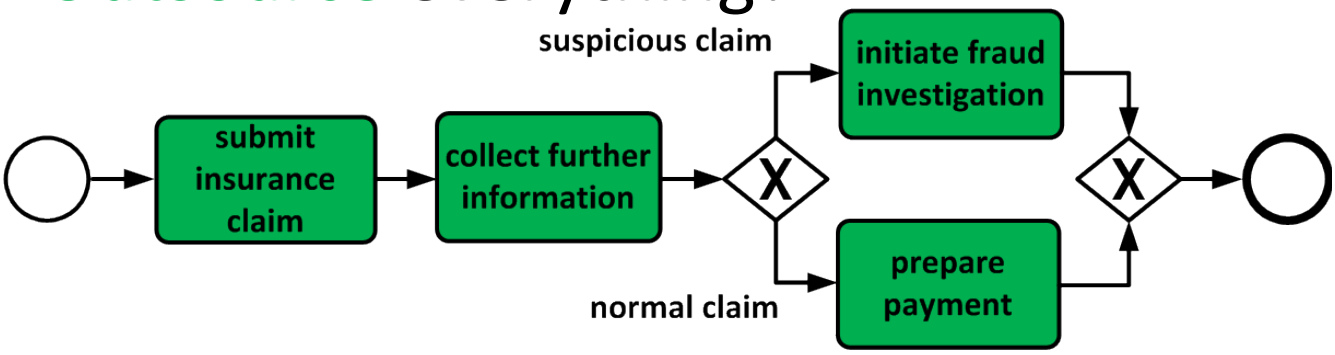
Confidential excludes outsourced.



Back to mission.

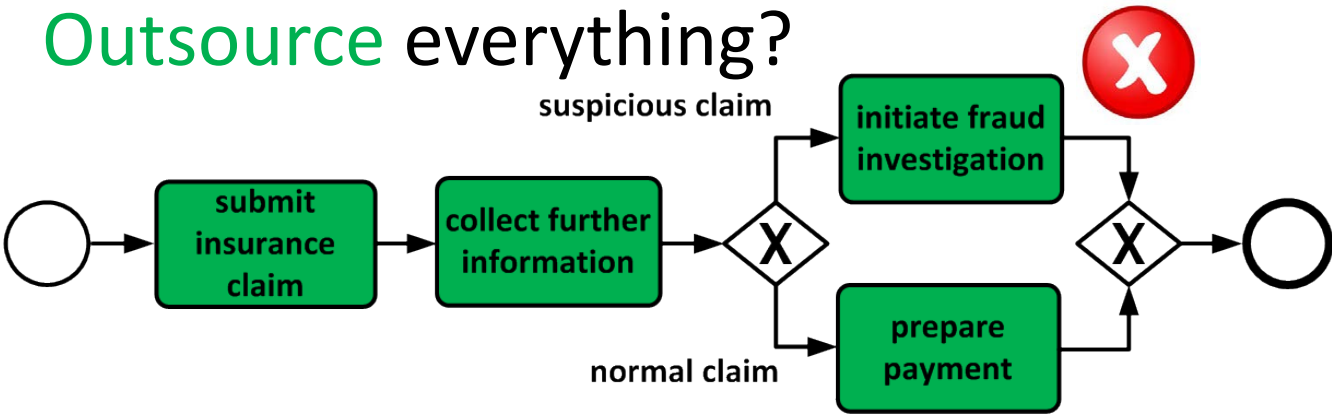
Mission accomplished? 8

Outsource everything?



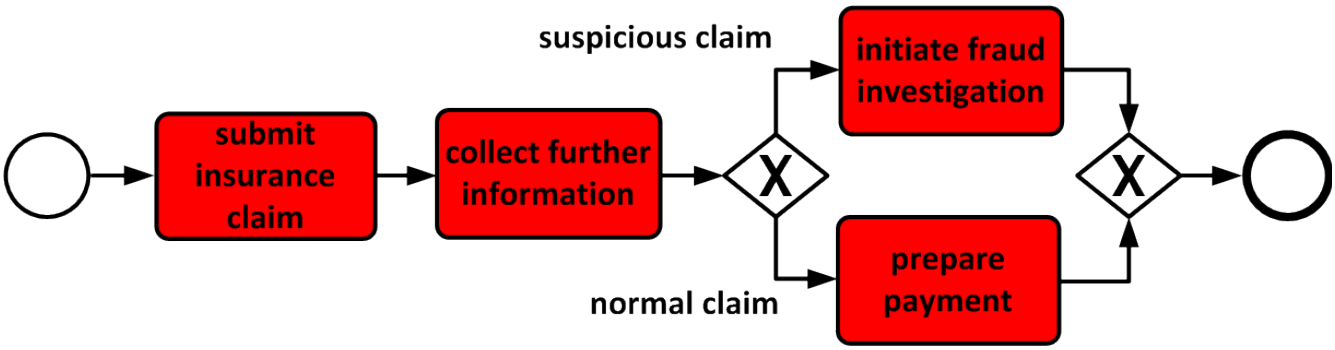
Mission accomplished? 8

Outsource everything?



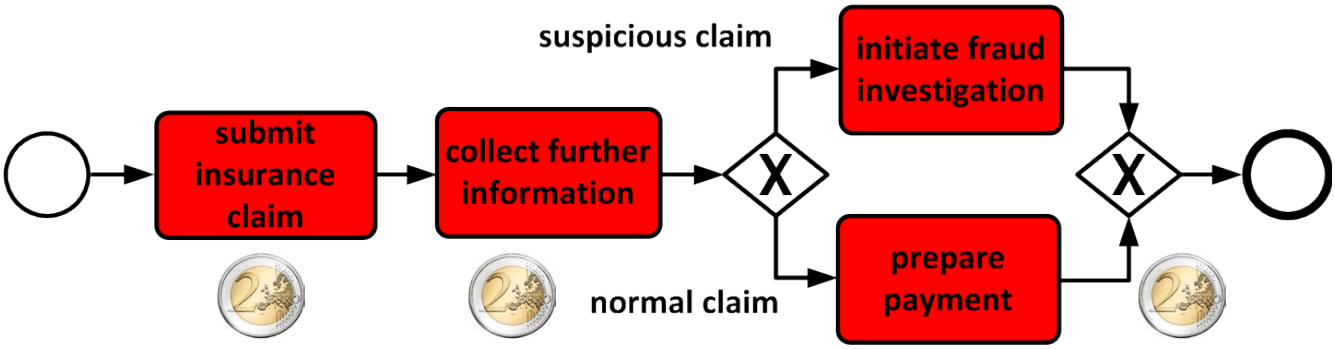
Mission accomplished? 8

Keep everything confidential?

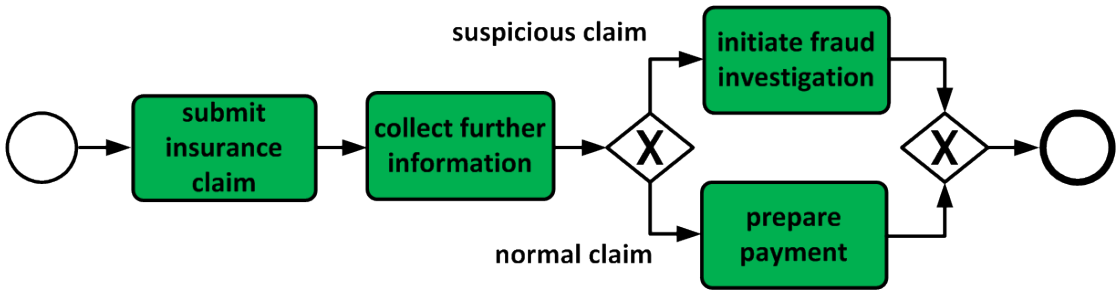


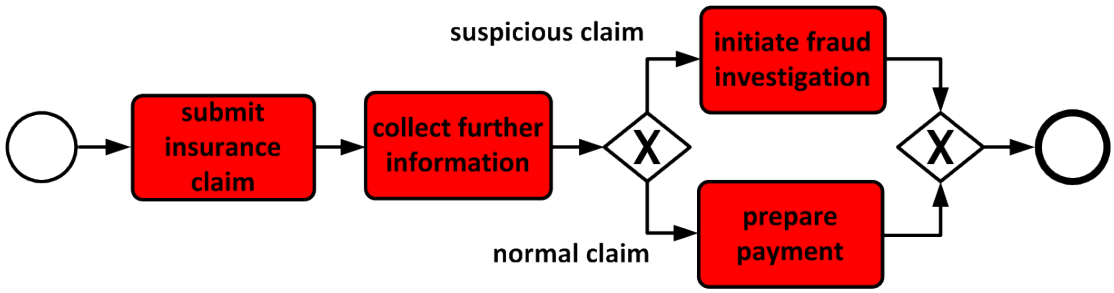
Mission accomplished? 8

Keep everything confidential?



Mission still open! 9





Mission still open! 9

2^t possible assignments

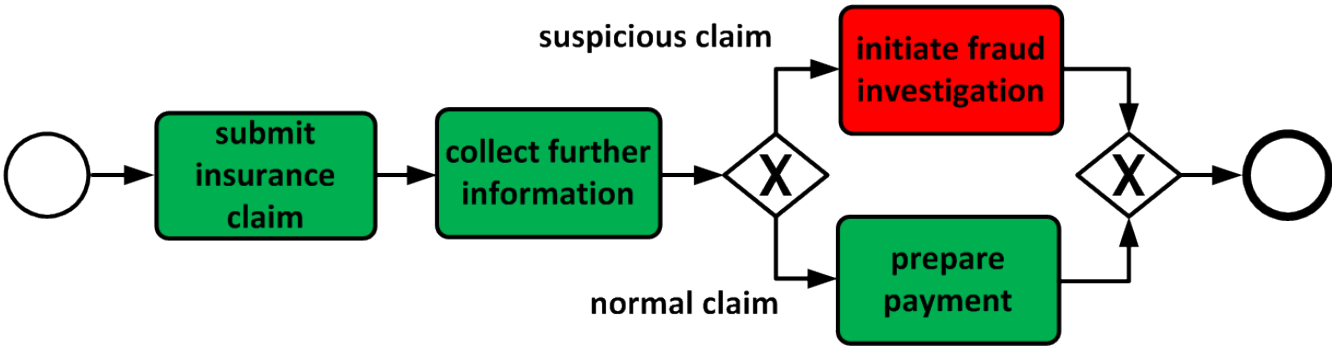
Mission still open!

2^t possible assignments

most task assignments are uninteresting

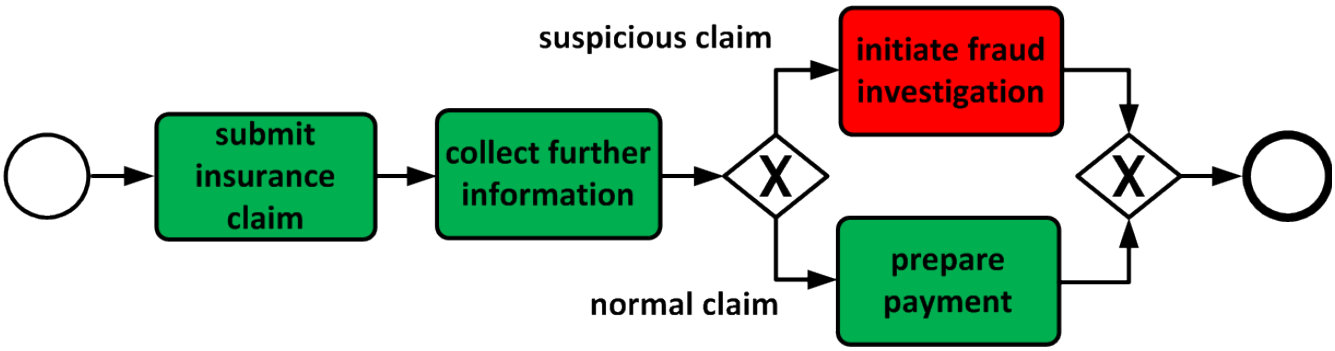
Model support

Model support: first try 10



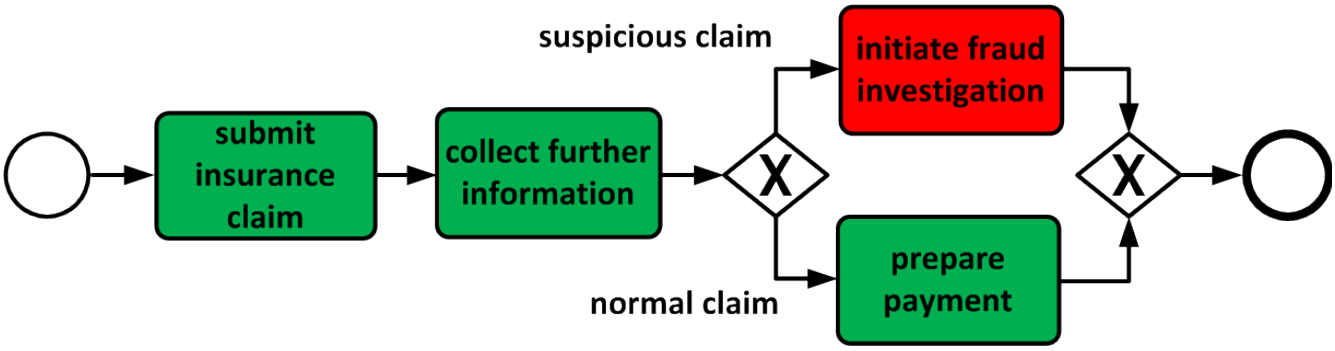
1. Assign **all** tasks.

Model support: first try 10



1. Assign **all** tasks
2. Press „Verification“.

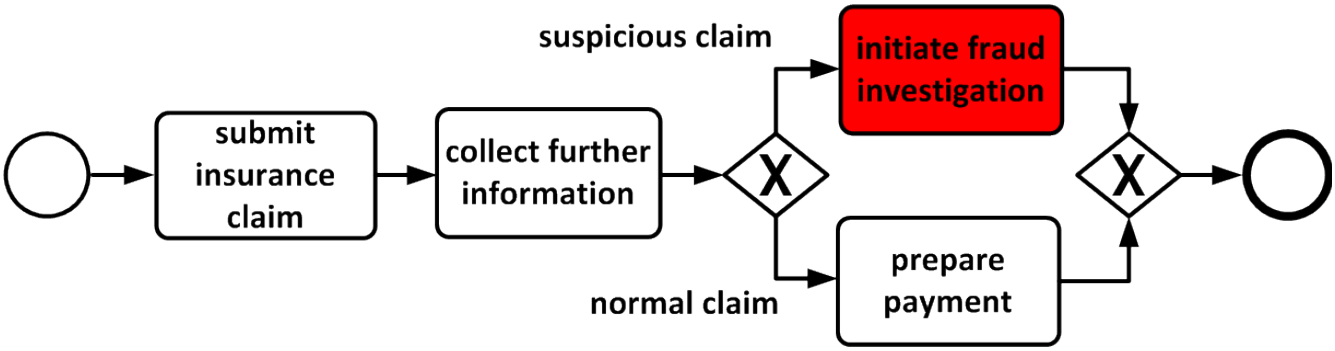
Model support: first try 10



1. Assign **all** tasks.
2. Press „Verification“.
3. Evaluate result.

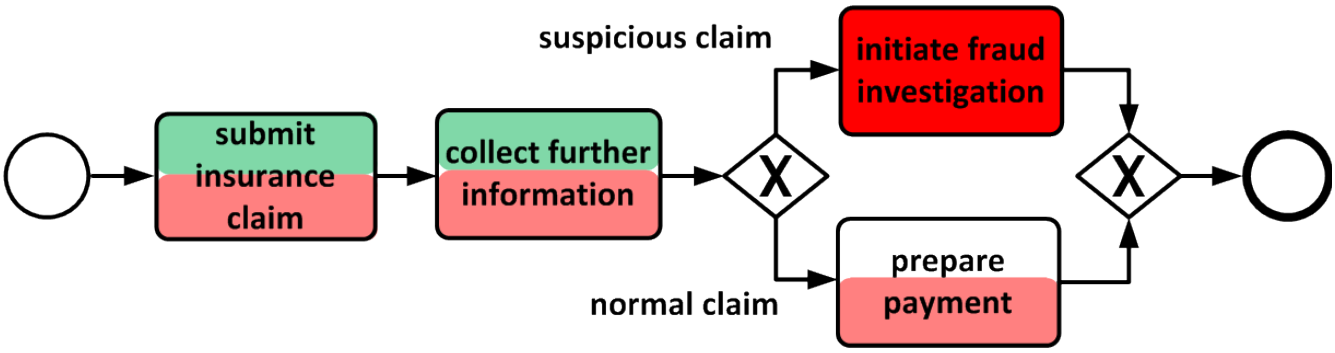
Problem: stupid and nerving (2^t options)

Model support: second try 11



1. Assign **confidential** tasks.

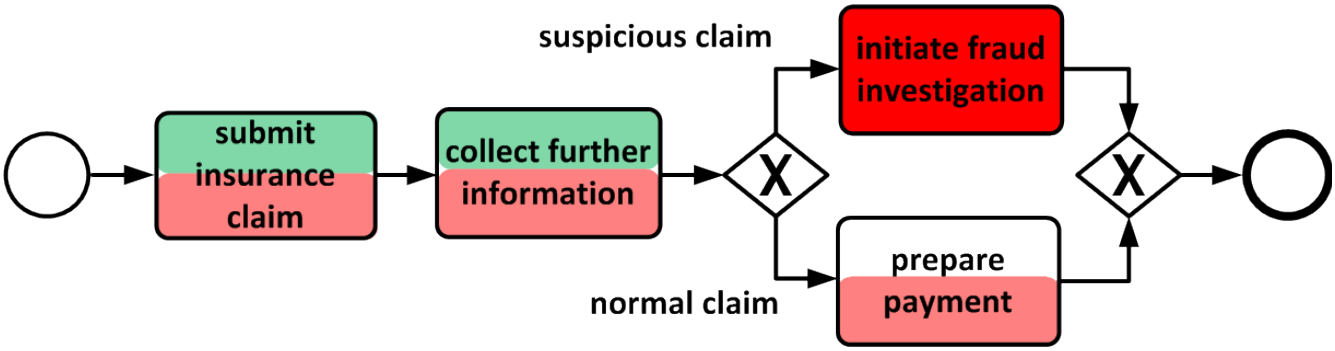
Model support: second try



1. Assign **confidential** tasks.
2. Assign restricted tasks.

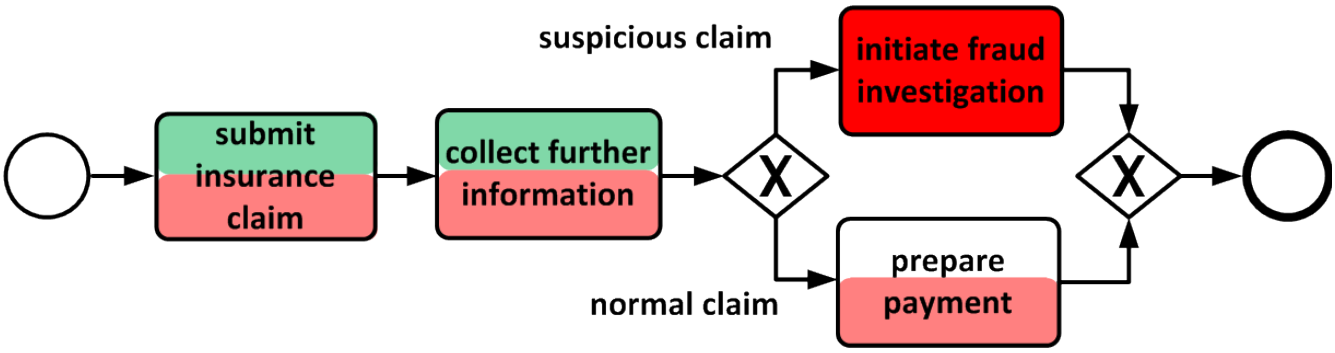
Model support: second try

11



1. Assign **confidential** tasks
2. Assign restricted tasks.
3. Assign all (other) tasks.

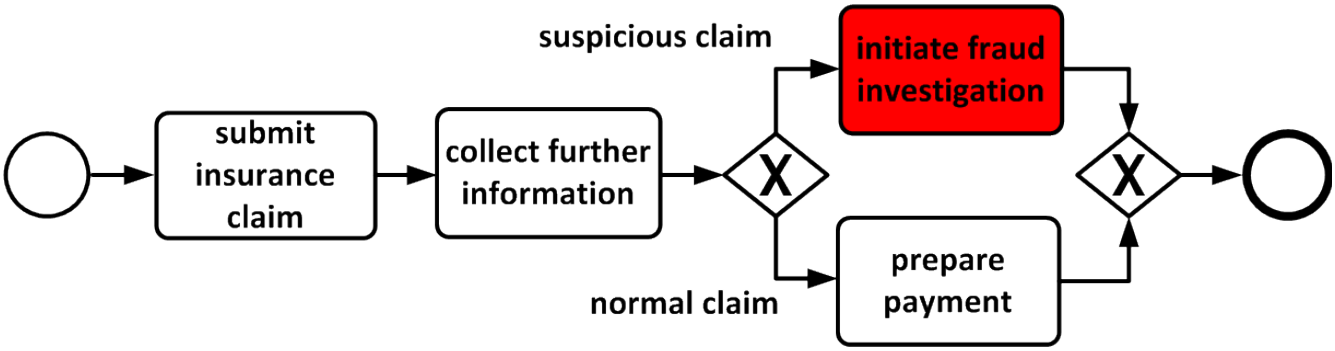
Model support: second try 11



1. Assign **confidential** tasks.
2. Assign restricted tasks.
3. Assign all (other) tasks.
4. Press „Verification“.

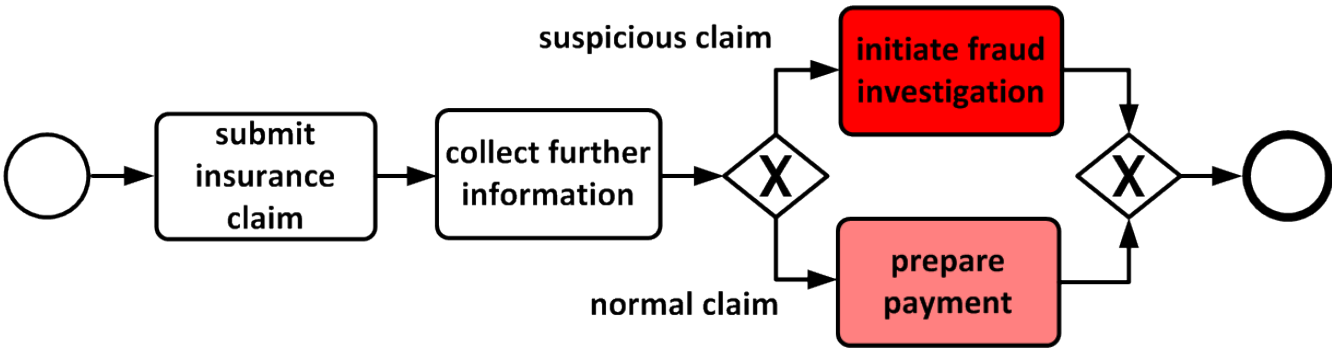
Problem: still nerving (~2^t options)

Model support: goal 12



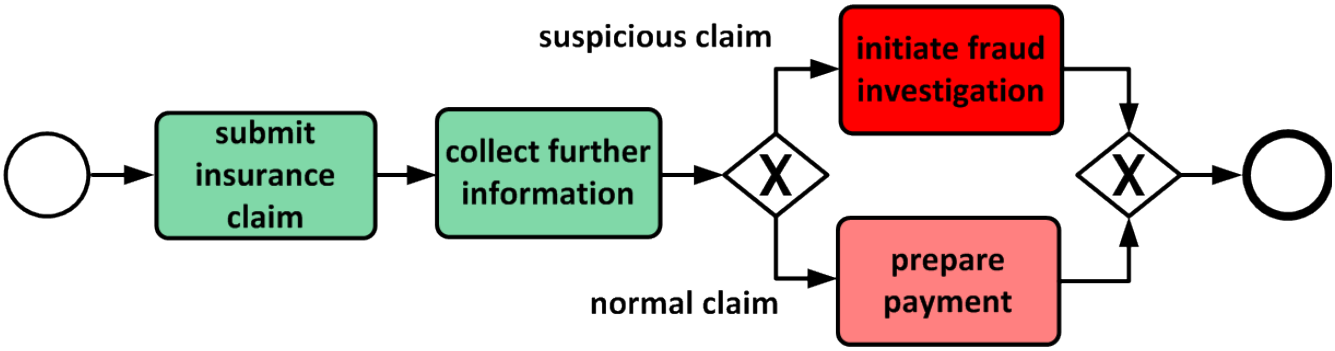
1. Assign **confidential** tasks.

Model support: goal 12



1. Assign **confidential** tasks.
2. Get all implied assignments.

Model support: goal 12



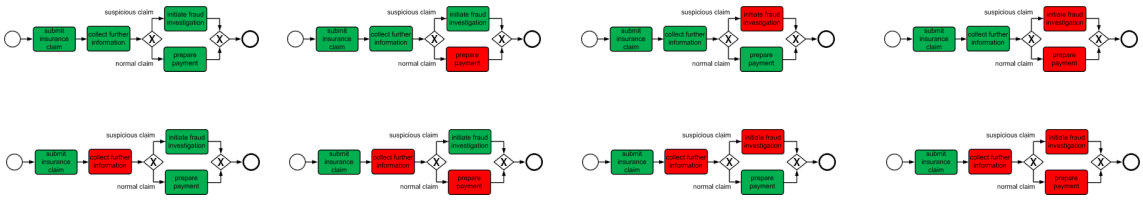
1. Assign **confidential** tasks.
2. Get all implied assignments.
3. Outsource as much as possible.

Confidentiality by design

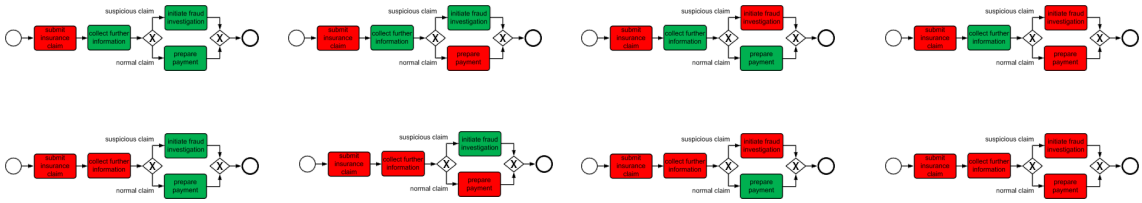
Confidentiality by design

Problems:
too many assignments

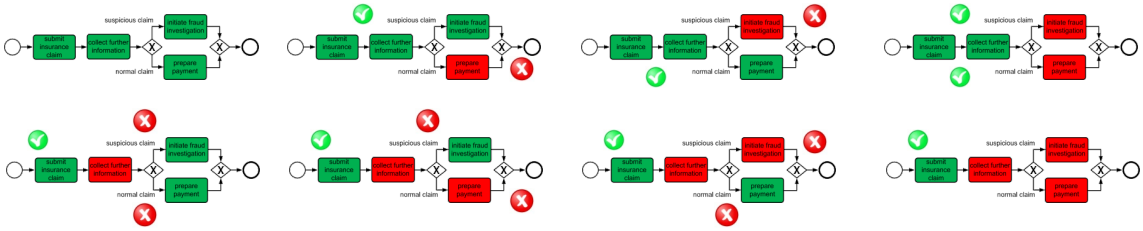
Confidentiality by design 13



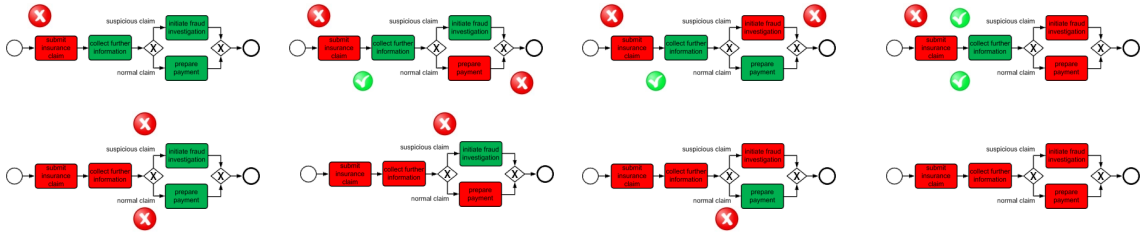
Problems:
too many assignments



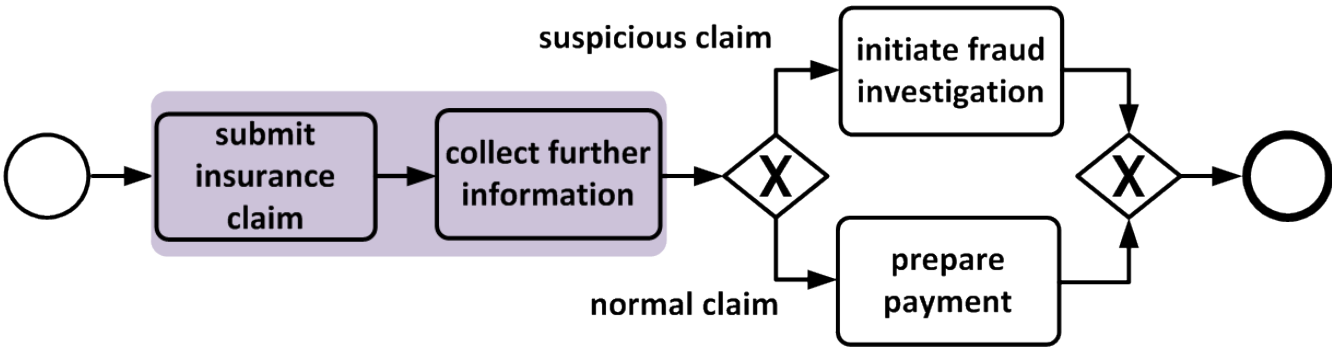
Confidentiality by design 13



Problems:
too many assignments
too many checks for them



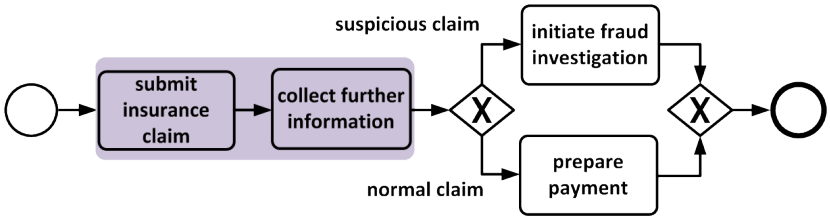
Checks are independent.



Depends „collect“ on „submit“?

Solve problems 14

Save contraints.



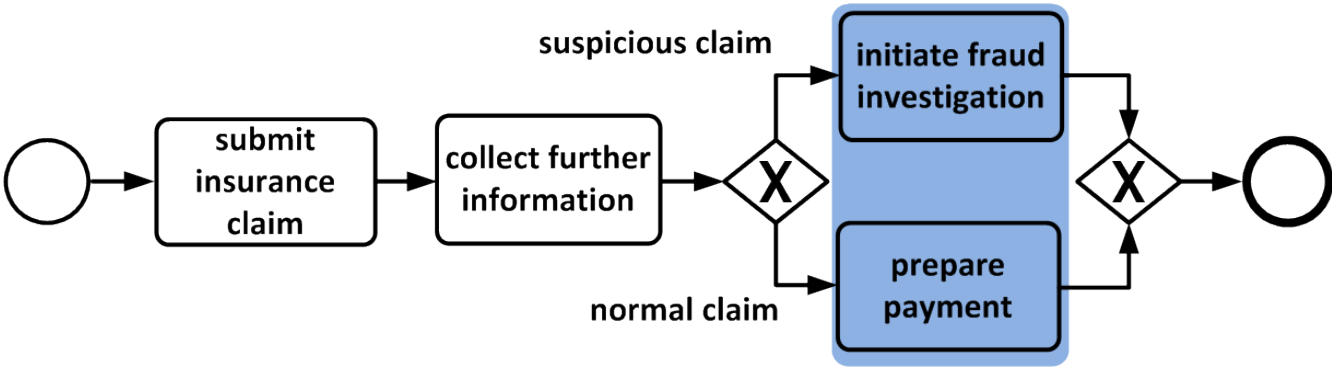
submit = high Λ collect = low

Constraint:

NOT (submit = high Λ collect = low)

Solve problems 14

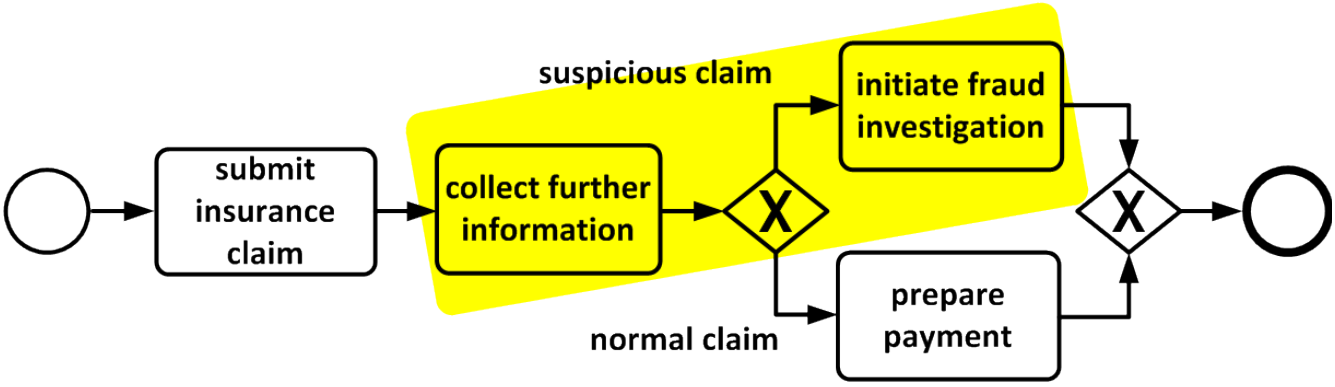
Checks are independent.



Mutual exclusion of „prepare“ and „initiate“?

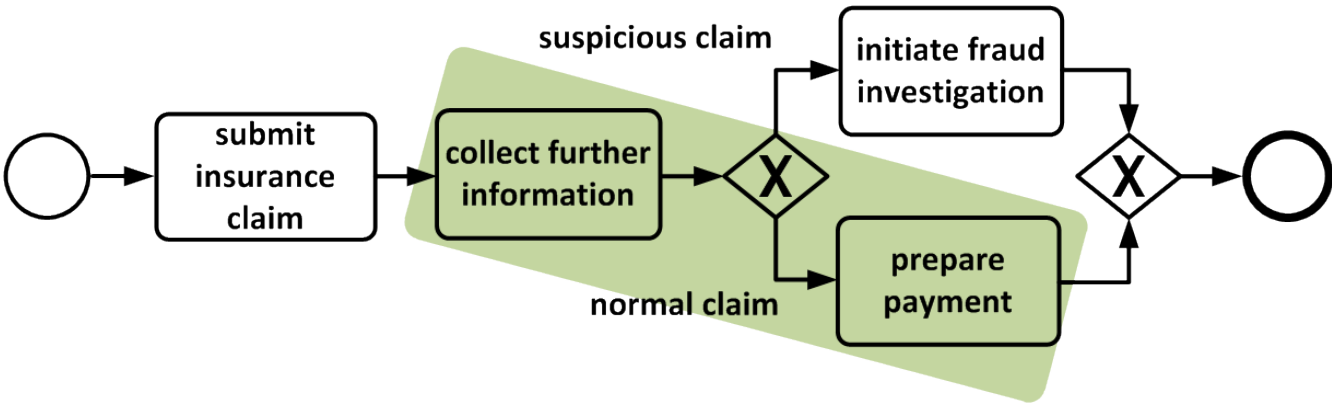
Solve problems 14

Checks are independent.



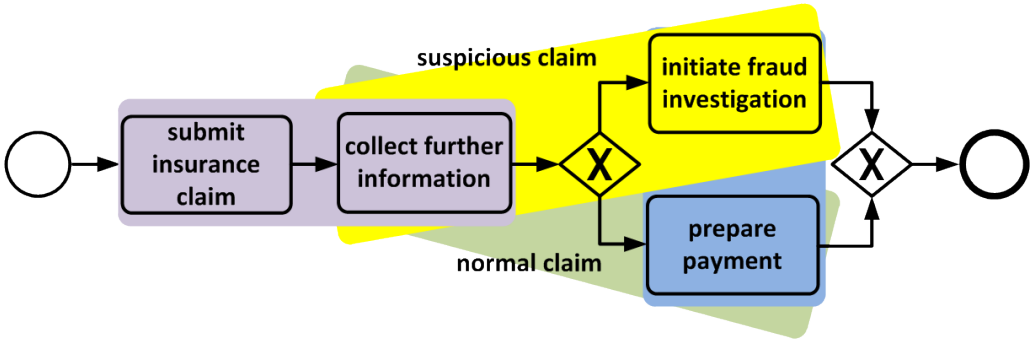
Depends „initiate“ on „collect“?

Checks are independent.



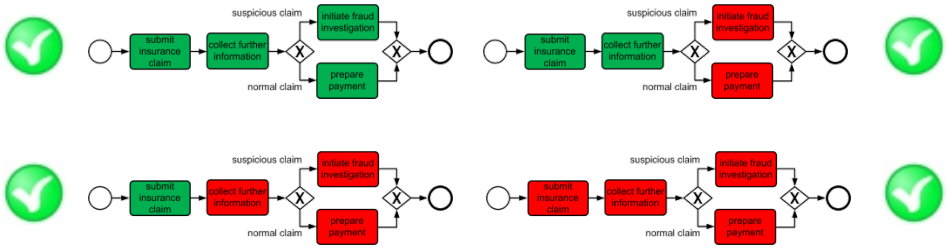
Depends „prepare“ on „collect“?

Solve problems 14

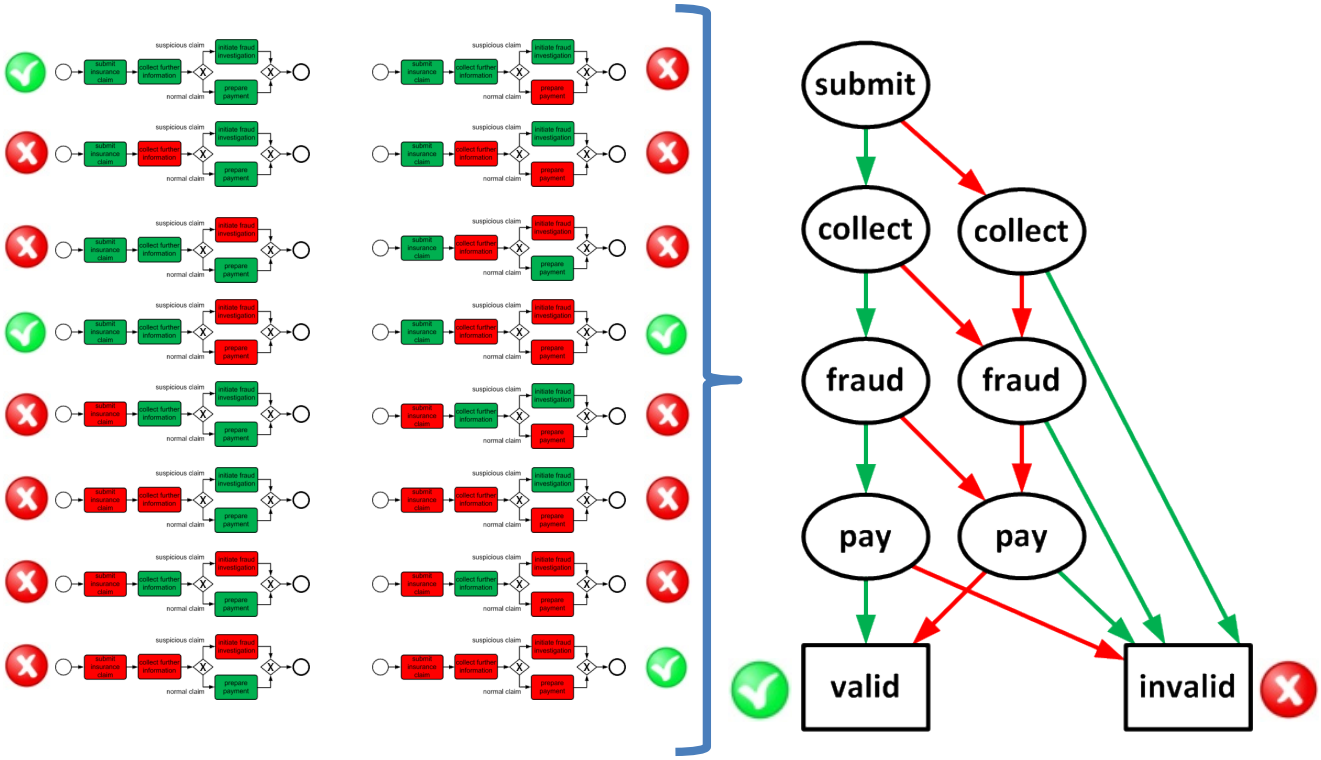


5 of 20 checks necessary

4 of 16 assignments are valid

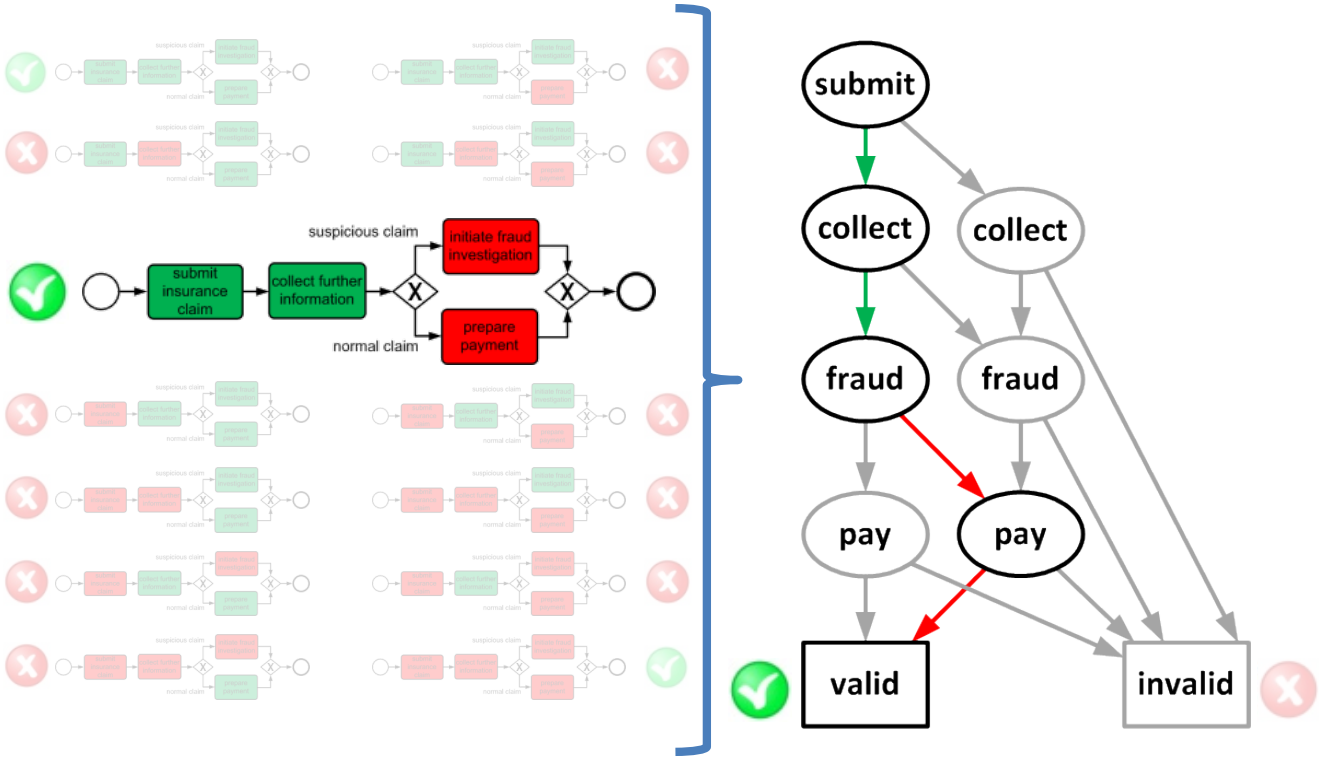


Represent assignments symbolically.



Solve problems 15

Represent assignments symbolically.

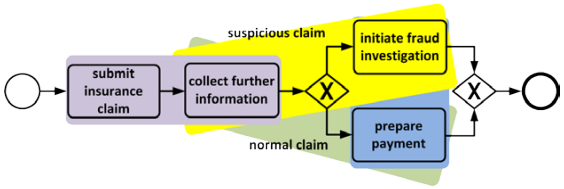


Evaluation

Confidentiality model support for 559 business processes

	Minimum	Average	Maximum
Tasks	1	20	100
Assignments	2	1,048,576	$> 10^{30}$

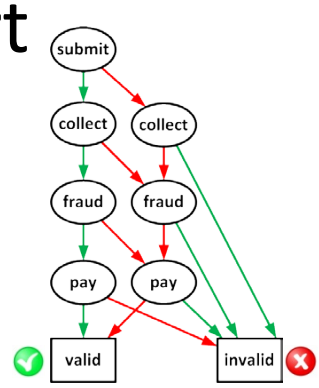
Confidentiality model support for 559 business processes



	Minimum	Average	Maximum
Tasks	1	20	100
Assignments	2	1,048,576	$> 10^{30}$
Checks	**3**	**38**	**282**

Evaluation 16

Confidentiality model support for 559 business processes



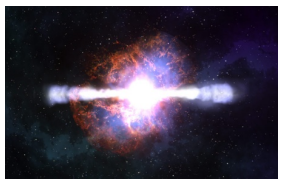
	Minimum	Average	Maximum
Tasks	1	20	100
Assignments	2	1,048,576	$> 10^{30}$
Nodes in BDD	**7**	**107**	**1,090**

Confidentiality model support for 559 business processes

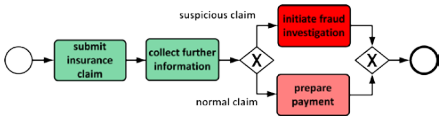
	Minimum	Average	Maximum
Tasks	1	20	100
Assignments	2	1,048,576	$> 10^{30}$
Checks	3	38	282
Nodes in BDD	7	107	1,090
Time (sec)	**0,00**	**0,09**	**2,14**

Take-Home Points

1 **Confidentiality is relevant.**
Protects sensitive assets.



2 **Confidentiality by design.**
Avoids subsequent verification steps.



3 **Confidentiality is practicable.**
Model and tool support

Take-Home Points

1 **Confidentiality** is relevant.
Protects s[illegible]

Tomorrow

Tool-Demo!

2 **Confidentiality** by design
Avoids subsequent
verification steps

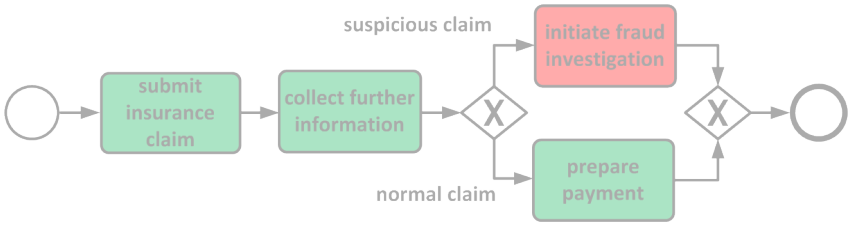
The day after tomorrow

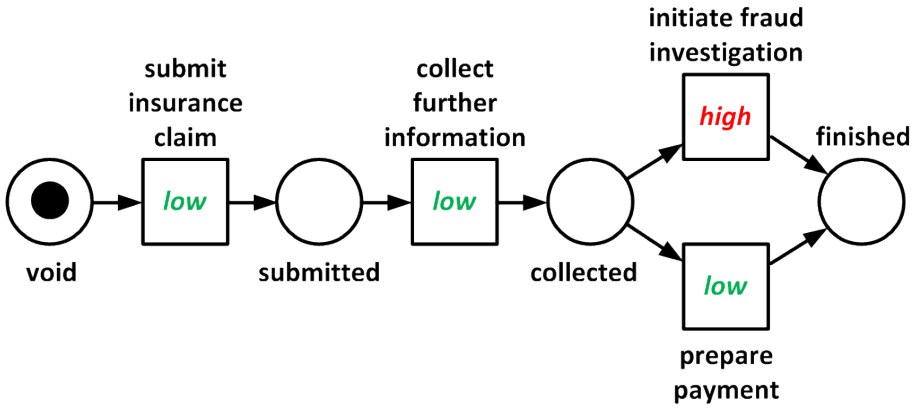
Verification background

3 **Confidentiality** is practicable!
Model and tool support

Backup

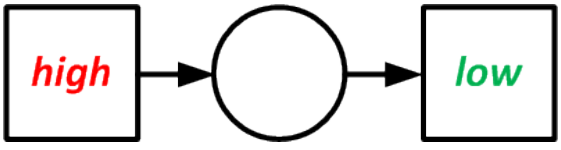
Formalism: Petri nets A

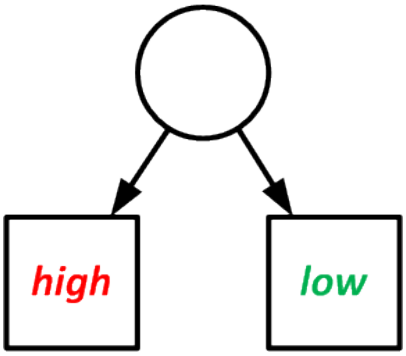




Formalism: Noninterference B

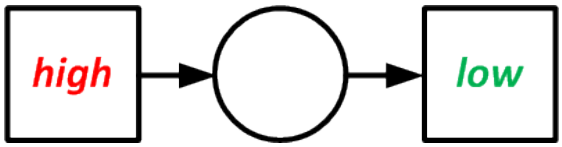
Positive Place Based Noninterference





Formalism: Noninterference B

A potential causal place…

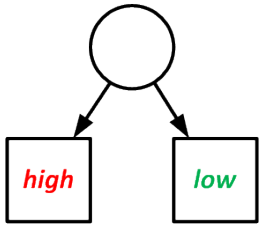


…is an active causal place:

High marks causal place.
Other transitions may fire.
(except those marking causal place)
Low is activated.

Formalism: Noninterference B

A potential conflict place…



…is an active conflict place:

High is activated in m.
Other transitions may fire from m.
(except those marking conflict place)
Low is activated.