



Nederlands Forensisch Instituut  
*Ministerie van Veiligheid en Justitie*

## Hansken job scheduler:

Definition of business rules  
according to the MBRM  
framework



Date: July 6th, 2012  
Supervisor: Dr. M. Worring (UvA)  
R. van Baar (NFI)



## Table of contents

- Introduction
  - Digital investigation process
- Problem definition
- MBRM method
- Business rules
  - Theory
  - Requirements
  - Rules
- Business rules management system (BRMS)
  - Requirement principles
- Conclusion
- Recommendations
- Questions





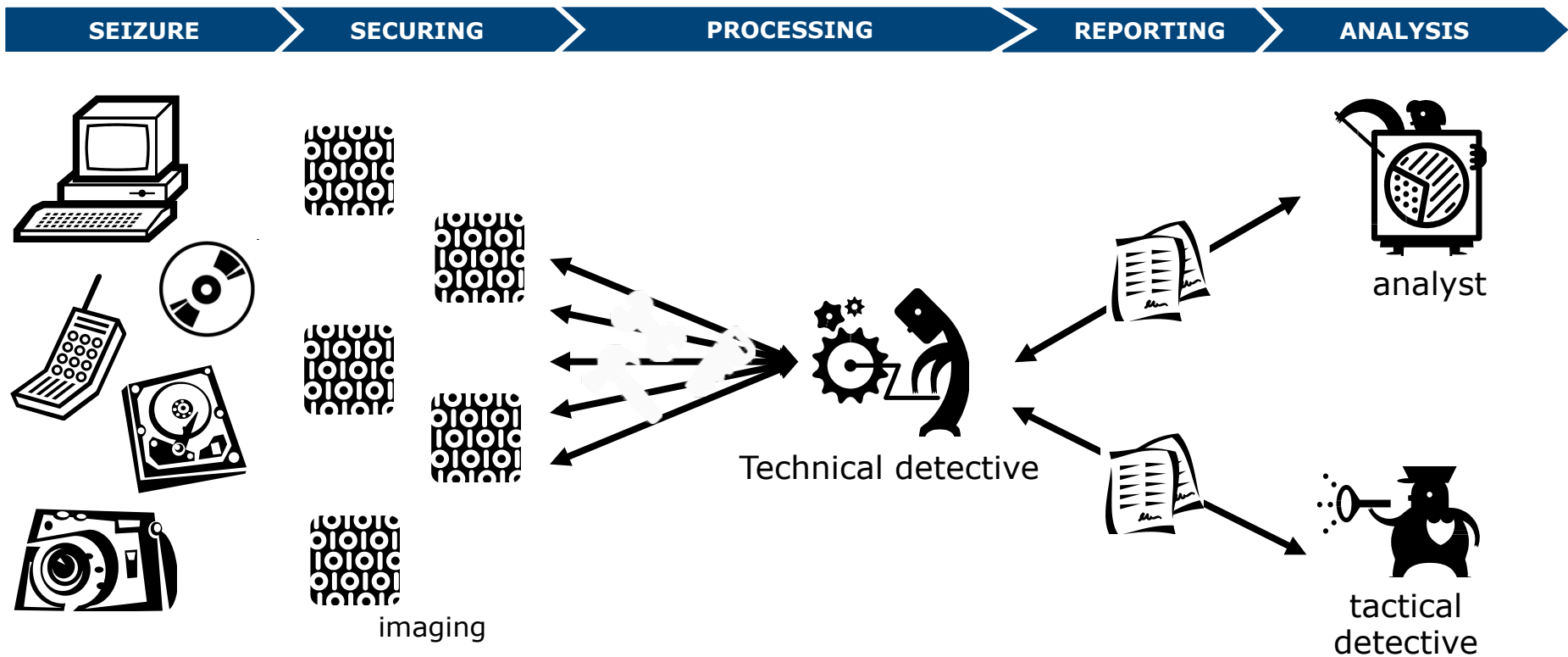
## Introduction: digital investigation, anno 2014:

In the Netherlands, based on current case statistics from the NFI:

Number of police agency's:	10
Cases:	1.000 per agency, per year
Average case size:	4.000 GB (min: 1MB, max: 200TB)
Retention time:	6 months
Storage capacity needed:	200.000.000 GB = 20.000 TB = <b>20 PB of case data a year</b> 8 Gb data-upload per second (resulting in 3 PB of trace indexes every year)
Data to process:	110.000 GB = <b>110 TB of case data a day</b> 15 Gb data processing per second (resulting in 16 TB of trace indexes a day)



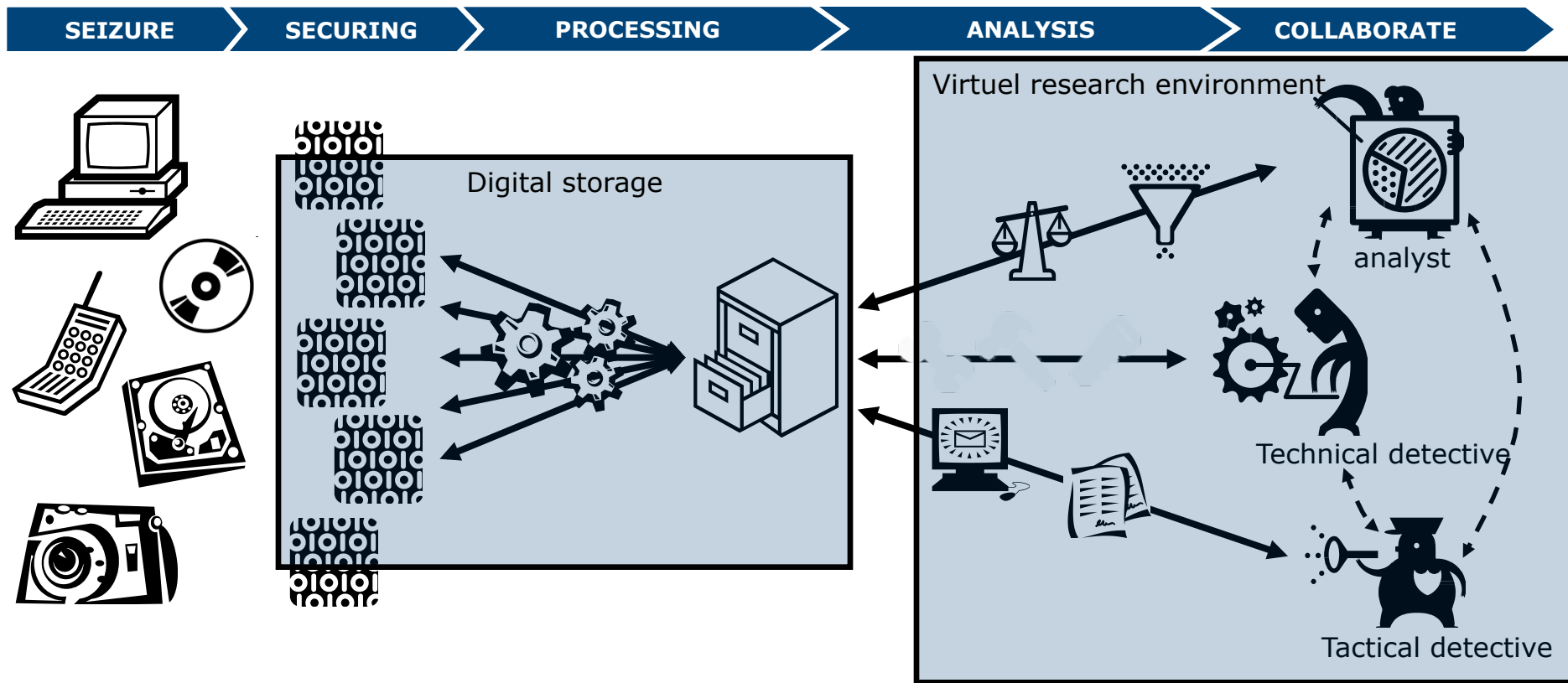
# The 'old fashioned' process of a digital investigation

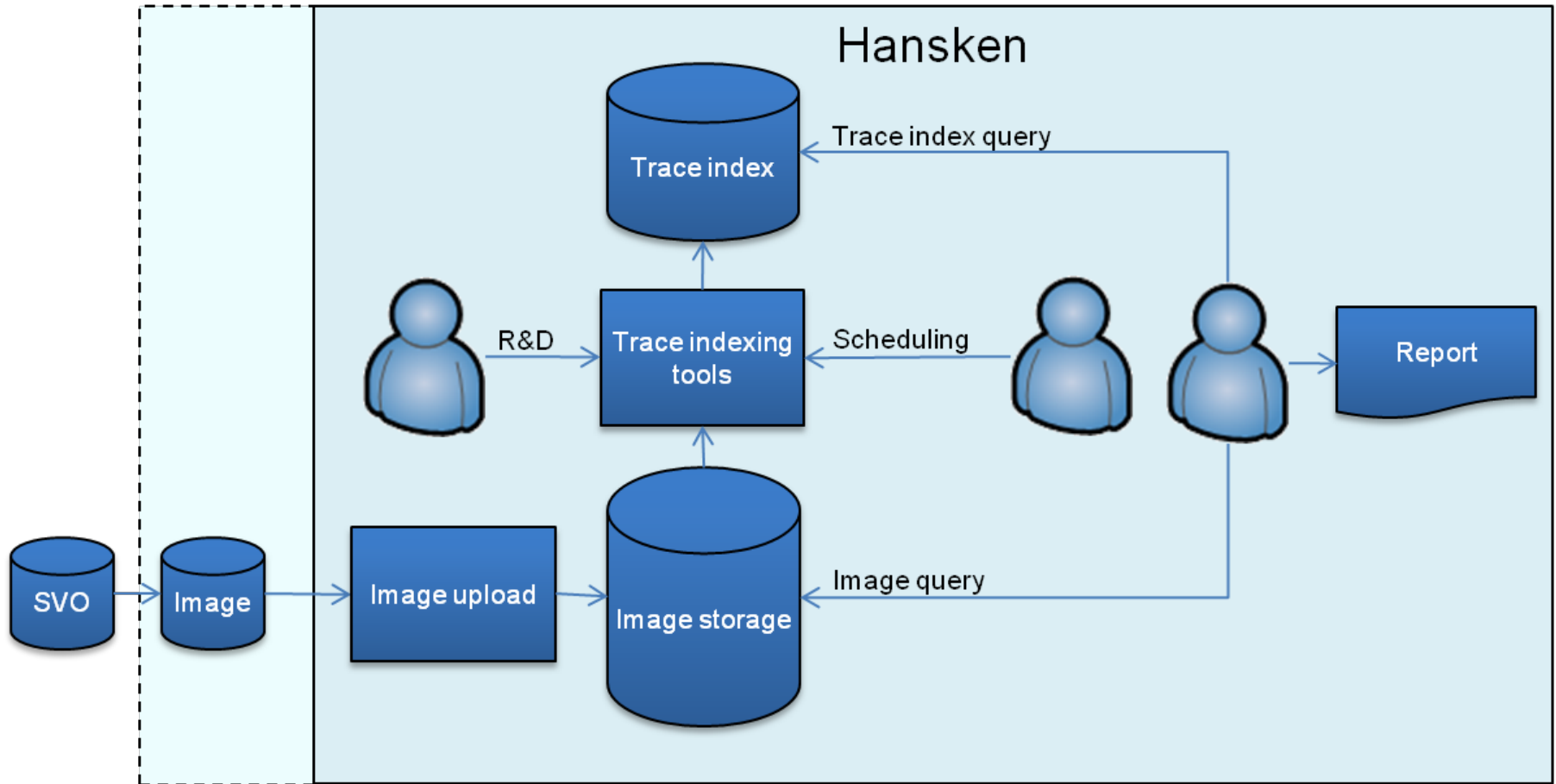




Save valuable time!

# The process of a digital investigation as a service







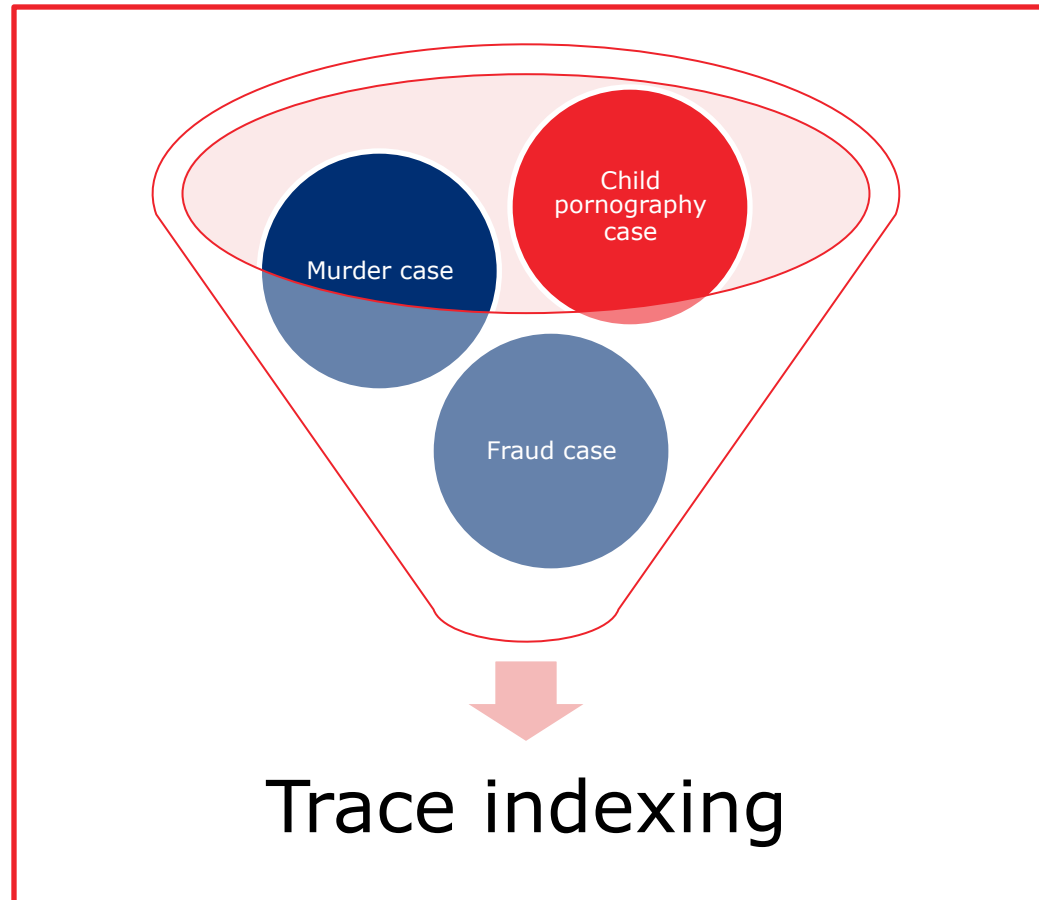
## Problem definition

- How should job scheduling principles be handled within Hansken?
  - Usage of business rules
    - How to capture and define business rules?
      - Methodology?
    - What rules should be defined?
  - Use a business rules management system (BRMS)!
    - What are its requirements?



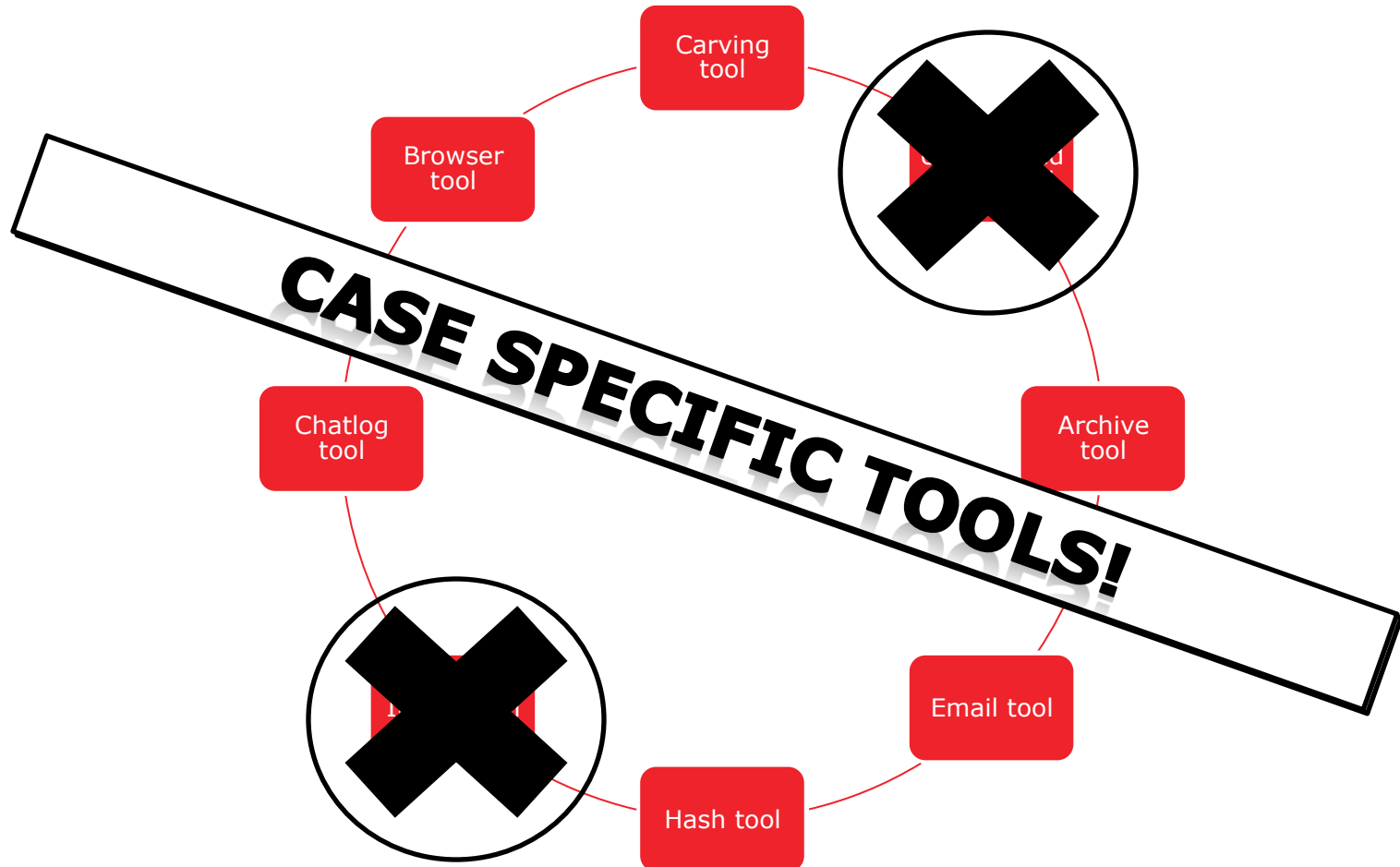


## Problem definition → an example





## Problem definition → an example (2)





## Problem definition → an example (3)



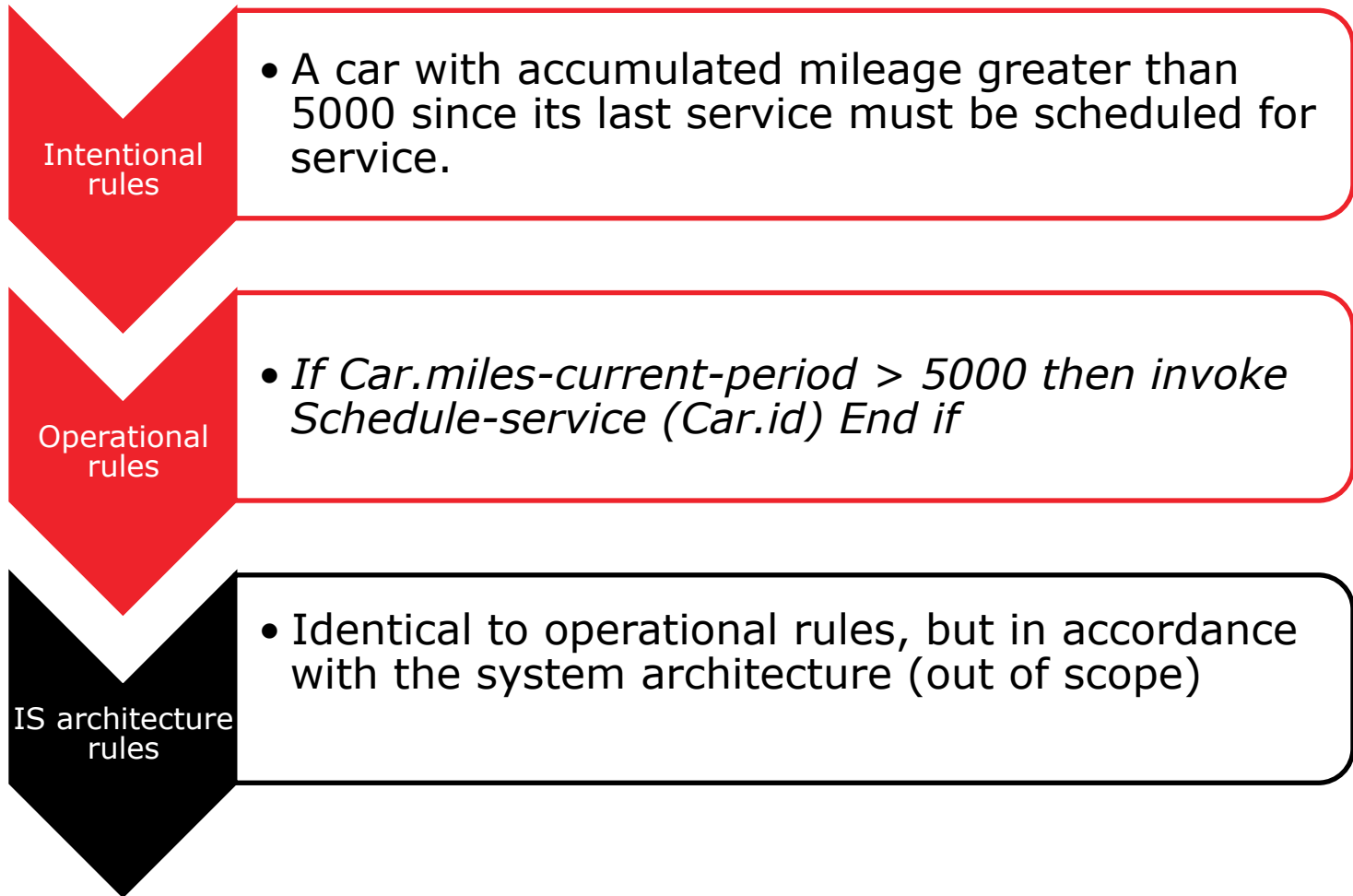


## Method

- Several rule management methods were assessed:
  - BRADES, SSADM and ERM-extensions but found to less suitable compared to MBRM.
- Usage was made of the Manchester Business Rule Management (MBRM) framework
  - Has proven its usefulness in similar large scale projects
  - Allows for **traceability** from rules to system components: transparency
  - Provides structural consistency for expressing and grouping rules



## Method

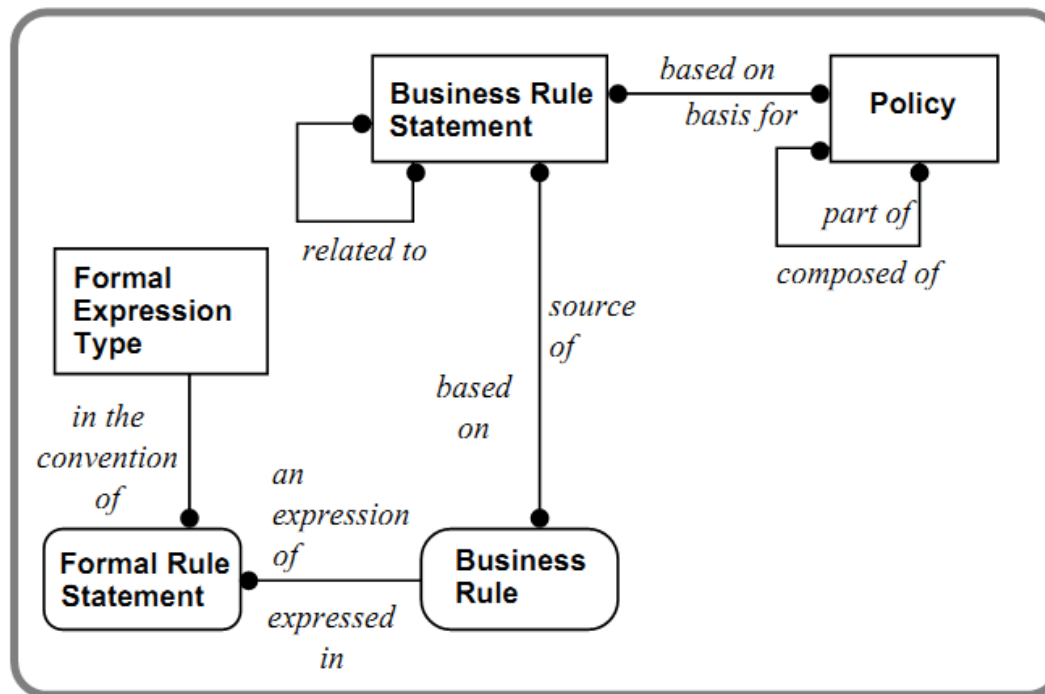




## Business rules - theory

*'Defines or constrains some aspect of a business'* – IBM

- Should aid the organization in achieving its goals
- Express policies within an organization using a formalized vocabulary





## Business rules – advantages

- Separate IT-architecture from variable business aspects
- Lowers the cost incurred in modification of business logic
- Rules are externalized, easily shared amongst applications
- Give rule authority back to business analysts
- Automation of business processes; save time



## Business rules

For what business processes must rules be applied?

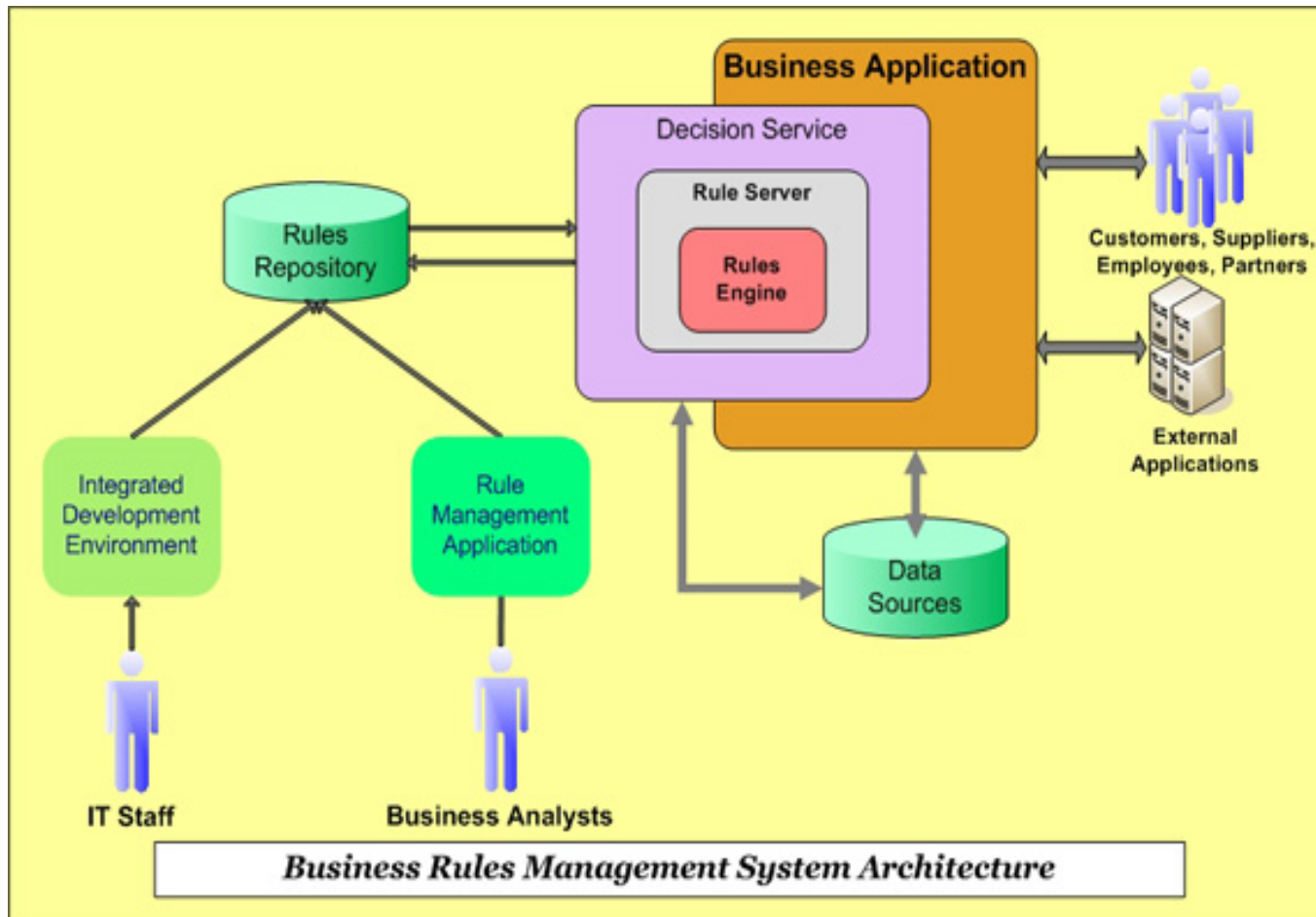
- Case priority
- Tool priority
- Case scheduling
- Quick indexing options
- Resource allocation / load distribution
- Priority themes
- Event job validation
- Alert generation
- Event logging → chain of evidence
- Trace indexing / a-synchronous query processing

```
if
    suspect hold time <=
    48 hours
then
    start quick scan
```





## Business rules management system - theory





## Business rules management system - requirements

The following requirement principles have been established:

- Privacy
- Security
- Reliability
- Transparency
- Stability
- Performance
- Compatibility
- Flexibility
- Scalability

- It is likely that the system will be implemented beyond The Netherlands



## Conclusion & recommendation

- This project has provided the NFI with a knowledge of:
  - How to capture and define business rules with the application of a scientific method
  - Specific set of business rule (statements)
    - How to manage business rules using a BRMS
- Operational rules → to IS-architecture rules → implementation
  - Format to RIF-standards (W3C) or vendor specific rule language (DRL, IRL)
  - Choice for a specific BRMS system, based on requirement principles



## Questions?

