Gemeente Rotterdam

Bart Ballaux

Jeroen van Oss

Building a risk based records management governance for the City of Rotterdam

DLM Forum, Lisbon

November 12th, 2014

Overview

- **Introduction, policy & governance**
- **Risk approach**
- **Records management regimes**
- **Implementation & conclusions**

Overview

- Introduction, policy & governance
- Risk approach
- Records management regimes
- Implementation & conclusions

Introduction

The setting

- Administration of approximately 11.000 civil servants
- \+ 500 business processes
- +1.000 software applications

-> *'The Wild West'*, < John MacDonald

Introduction

- Several attempts to introduce *proper* records management
- Departments responsible for records management
- Centralization -> opportunity to change
- Application-driven implementation of records management

Policy & governance

- **Records management is primarily the responsibility of the business**
- **Records management (like information security) is part of each business process**
- **Introduction of risk assessment**

Policy & governance

- **Records management *one* of the information fields, with information security, collaboration, business intelligence, open data, etc.**

- **Roadmap for each information theme**

    1. Policy & integration in information architecture
    2. Records management in IT systems
    3. Records management in business process re-engineering
    4. Organizational culture – awareness of value of information

Policy & governance

- **Records management *one* of the information fields, with information security, collaboration, business intelligence, open data, etc.**

- **Roadmap for each information theme**

1. Policy & integration in information architecture
2. Records management in IT systems
3. Records management in business process re-engineering
4. Organizational culture – awareness of value of information

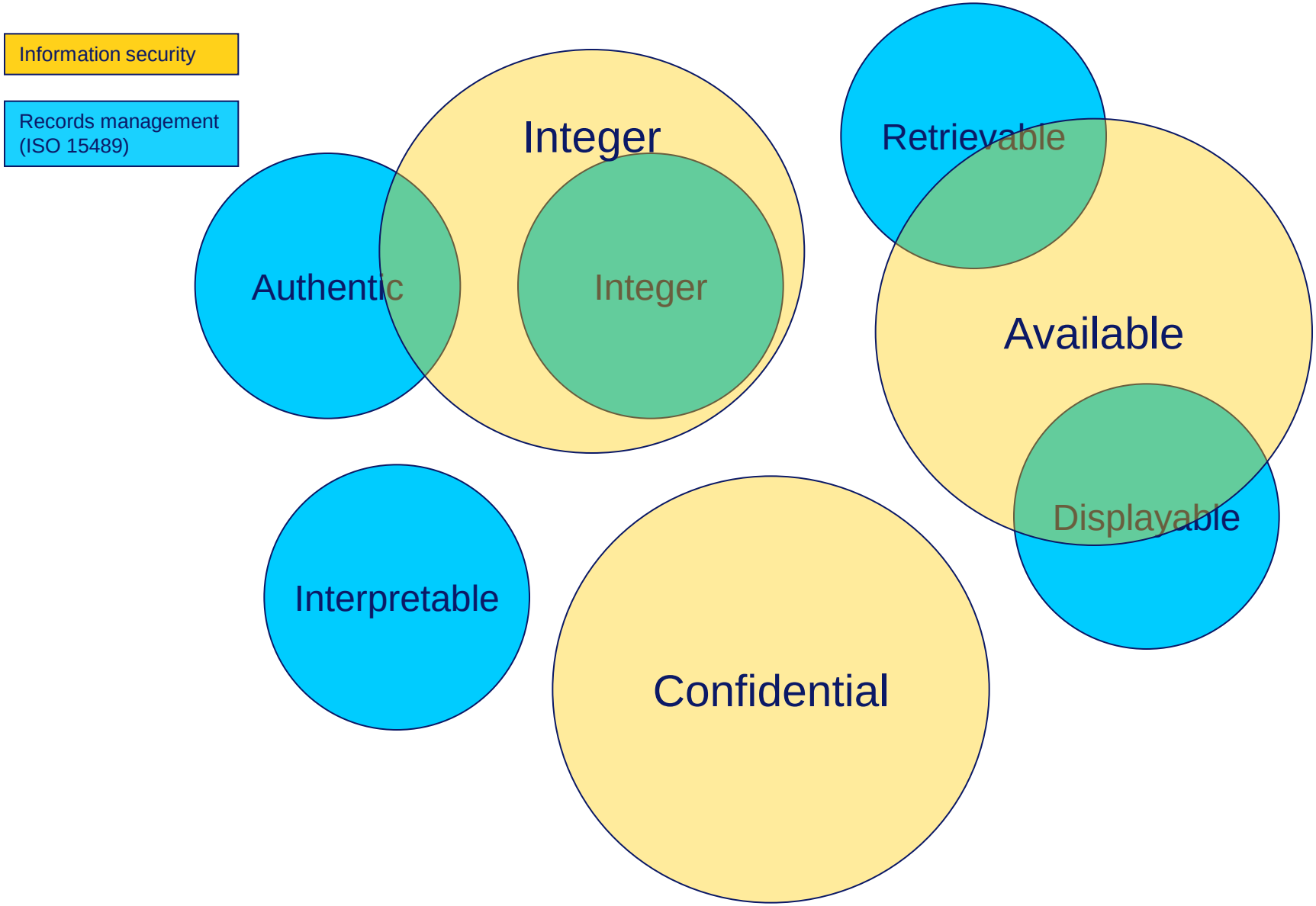
Overview

- **Introduction, policy & governance**
- **Risk approach**
- **Records management regimes**
- **Implementation & conclusions**

Risk approach: principles

- **Quality level of records management regime is determined by business *needs & risks***
- **Based on the importance of business *process & information***
- **Leads to an *appropriate level* of records management measures**

Risk approach: criteria



Risk approach: quality levels per criterion

Level	Authentic and integer
0	*Not sure*: the business process allows that there is no guarantee that the information is authentic and integer.
1	*Protected*: a basic level of guarantee for authenticity and integrity is required
2	*High*: the business process allows little violation related to authenticity and integrity.
3	*Absolute*: conclusive evidence about author, moment of creation, content, and changes, is necessary.

Risk approach: quality levels per criterion

Level	Retrievable
0	*Not necessary*: information may not be retrieved, without any consequence.
1	*Necessary*: information may incidentally not be retrieved.
2	*Important*: if necessary, information can be retrieved with special (incidental) effort.
3	*Essential*: information can be retrieved in a timely and efficient manner.

Risk approach: quality levels per criterion

Level	Interpretable
0	*For those directly involved*: persons directly involved are able to interpret and understand the information.
1	*For a broader group in the organization*: information can be interpreted and understood by persons not directly involved in the process, shortly after closure of the case.
2	*For users outside the organization and through time*: information can be interpreted and understood by users outside the organization and after closure of the case.
3	*For users at a large distance in space and time*: information can be understood and interpreted by persons and stakeholders who are at a great distance from the original business process and its information.

Risk approach: quality levels per criterion

Level	Displayable
0	*Not necessary*: information cannot be displayed without any consequence, even not by authorized persons.
1	*Necessary*: information cannot be displayed incidentally, even not by authorized persons.
2	*Important*: if necessary, information can be displayed with special (incidental) effort.
3	*Essential*: information can always be displayed by authorized persons.

Risk approach: from assessment to implementation

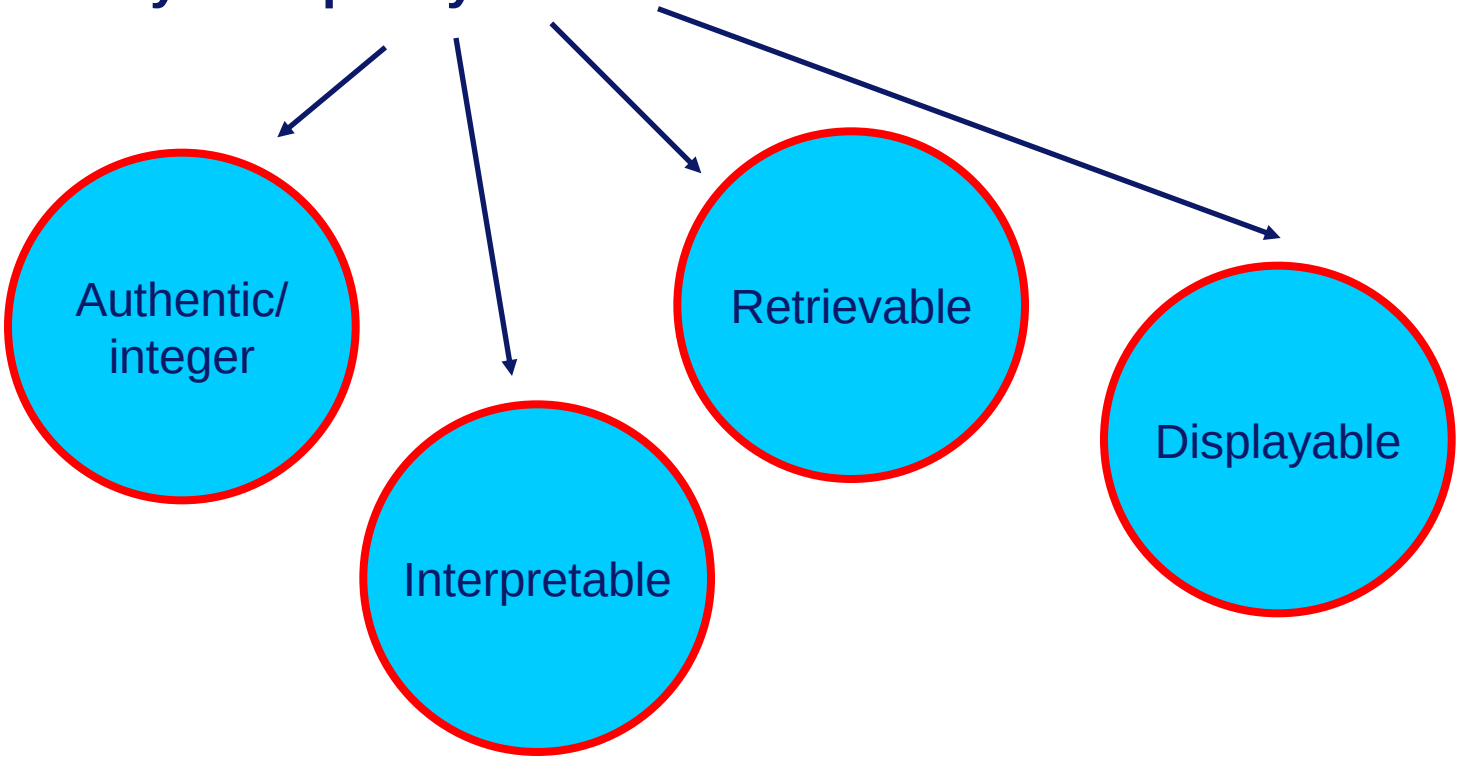
1. Filling risk tool with business owner

2. Determining classification level (0-3)

3. Implementing appropriate records management measures

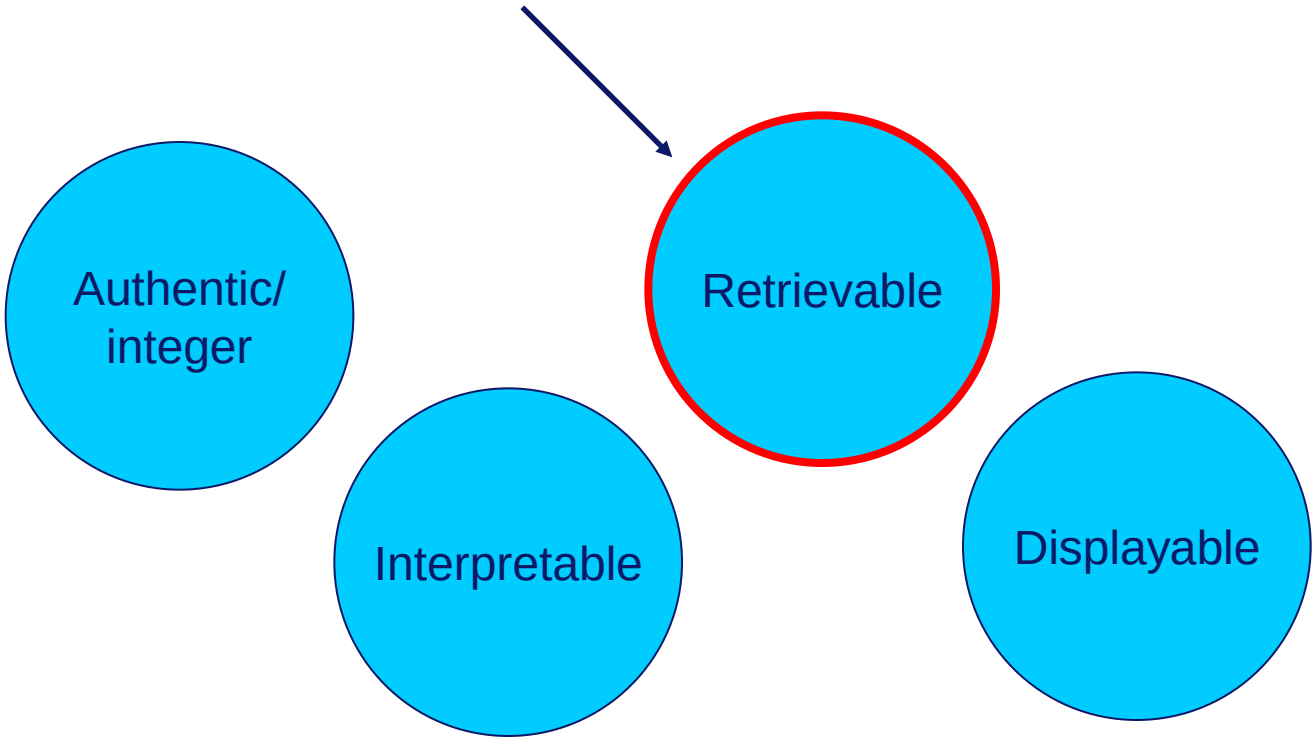
Risk approach: indicators & questions

Impact of financial, political, reputational or health risks caused by bad quality of information



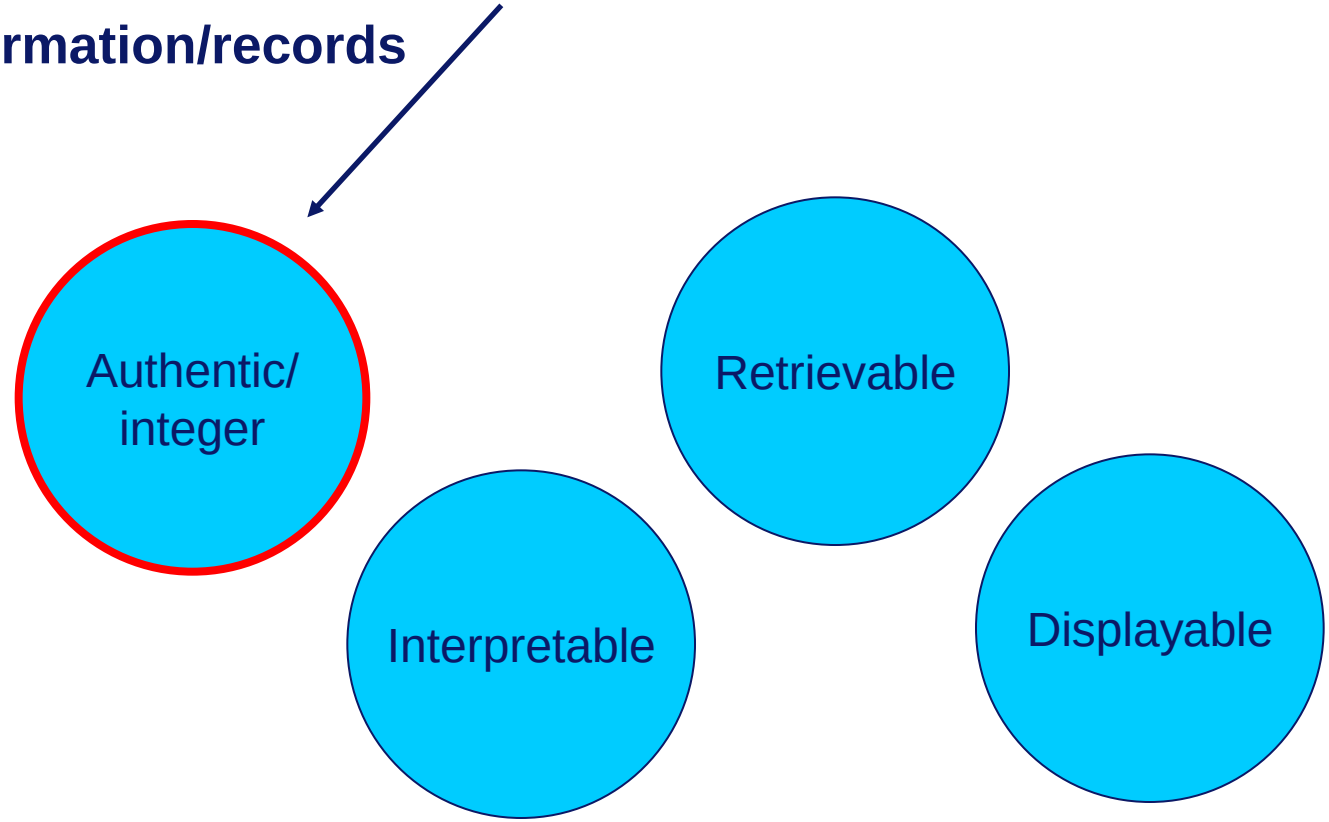
Risk approach: indicators & questions

Legal requirements related to the process, timely delivery



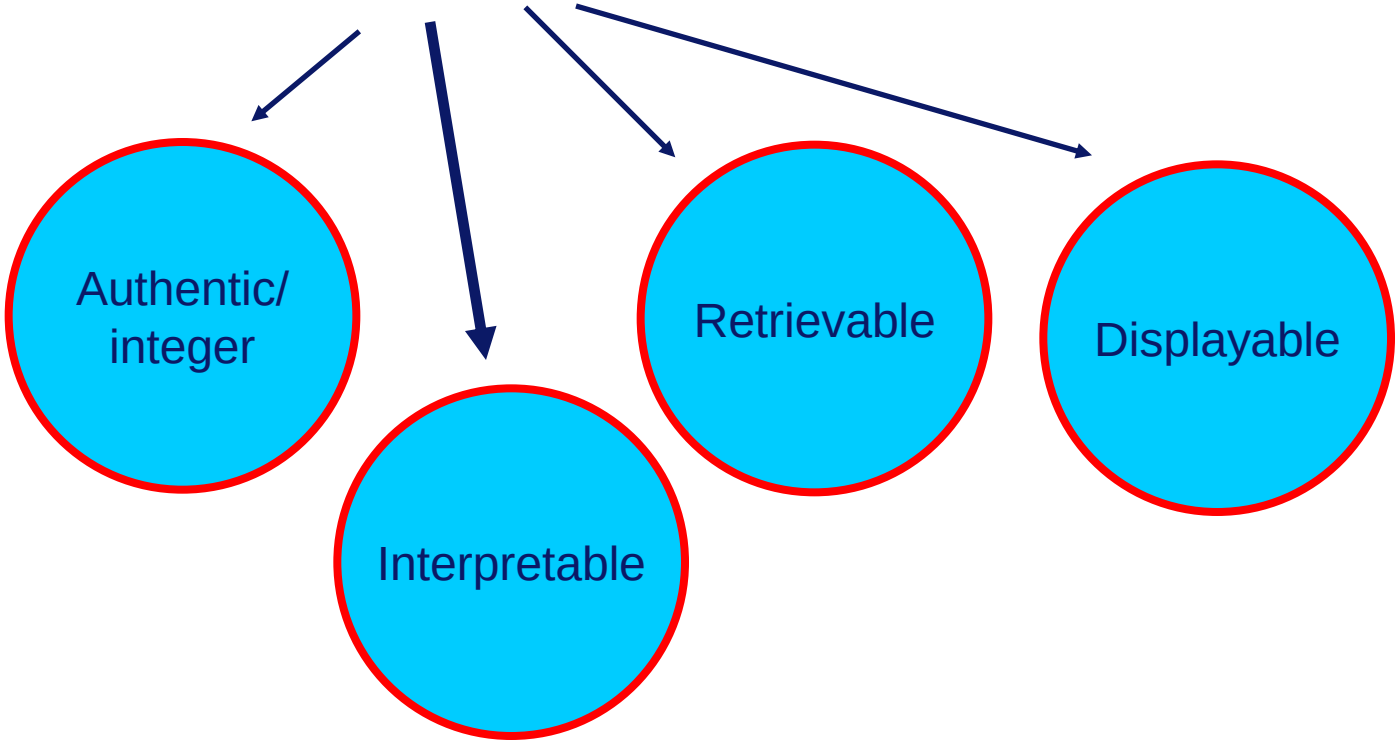
Risk approach: indicators & questions

Legal requirements related to the form and status of information/records

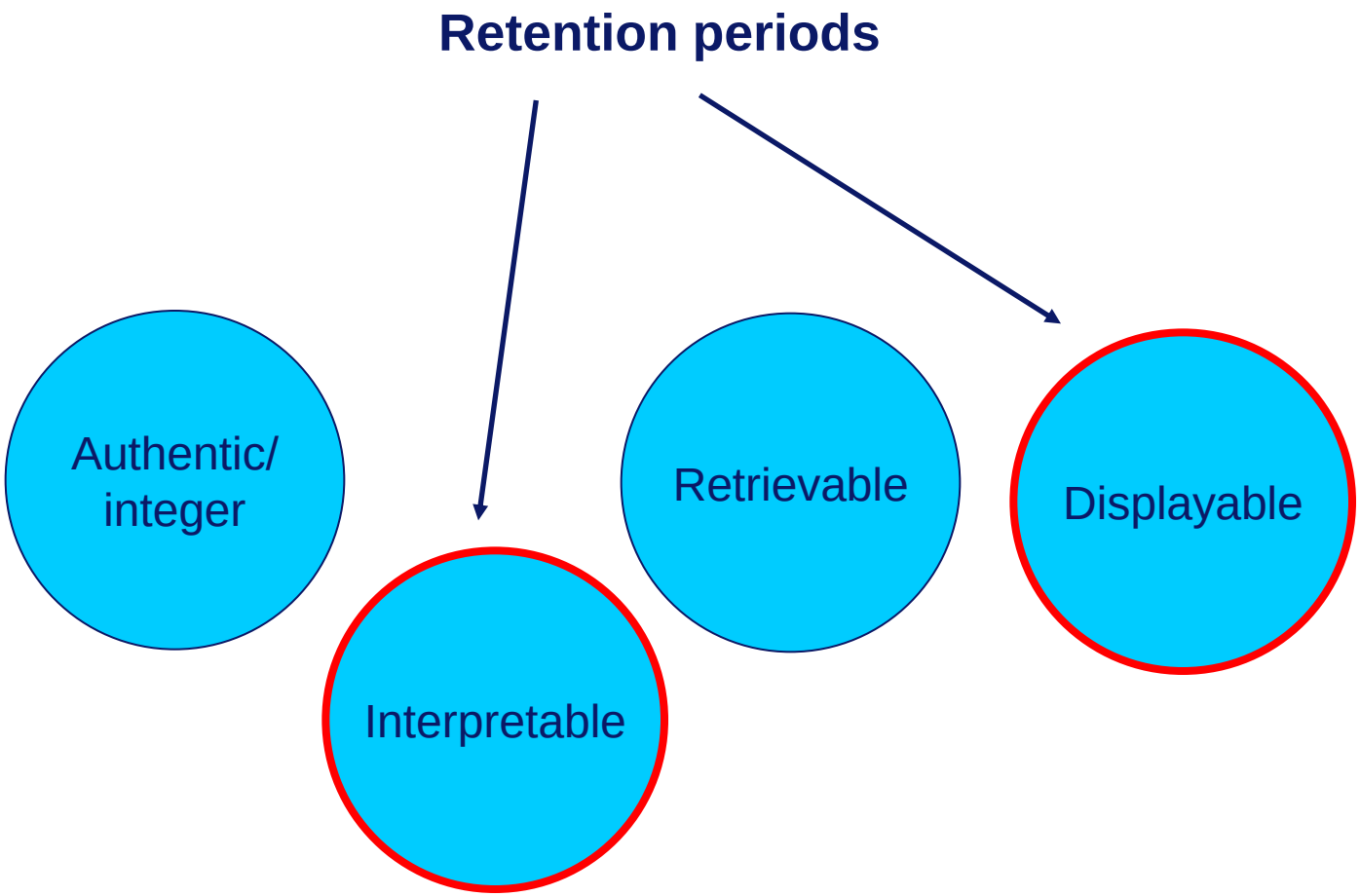


Risk approach: indicators & questions

The extent to which partners, law enforcers or accountants have to rely on information in a later phase



Filling the risk tool: indicators and questions



The risk tool: classification level determined

Authenticity/ integrity	Retrievability	Displayability	Interpretability	Classification
17pt=3	19pt=3	19pt=2	14pt=3	3

Overview

- **Introduction, policy & governance**
- **Risk approach**
- **Records management regimes**
- **Implementation & conclusions**

Records management regimes

- **Three fields of records management measures**
  - Metadata -> applications (<ISO 23081)
  - Functional requirements -> applications (<ISO 16175)

    => part of process re-engineering & architecture

  - Procedures -> organizational culture

    => part of educational task of records managers

- **Level 3: full set of requirements**
- **Level 0: no requirements**

Records management regimes: example 1 (metadata)

- **Metadata about place that relates to record, file or series**
    - Level 0 & 1: not necessary
    - Level 2: if applicable, necessary
    - Level 3: always necessary
- **Metadata about integrity check**
    - Level 0 & 1: not necessary
    - Level 3 & 4: always necessary

Records management regimes: example 2 (requirements)

- **Deletion of records, files & series should take place on the basis of metadata**
  - Level 0 & 1: not necessary
  - Level 2 & 3: mandatory
- **A record can only be added once to a file or series**
  - Level 0 & 1: not necessary
  - Level 2 & 3: mandatory
- **Unauthorized changes cannot be made**
  - Level 0 & 1: not necessary
  - Level 2 & 3: mandatory

Overview

- **Introduction, policy & governance**
- **Risk approach**
- **Records management regimes**
- **Implementation & conclusions**

Implementation

- Approximately 50 processes analysed

- Most of them in higher risk levels (2 & 3)

+ Awareness for records management in general is increasing

+ Records management is on the *radar* of managers

− Implementing in applications remains a technical challenge

− Convincing all employees takes a long period

Conclusions

- **Risks for business, not necessarily detailed records management risks**

- **Risk approach as a means to create awareness in organisation**

http://www.stadsarchief.rotterdam.nl/informatiebeheer/instrumenten