

**Author(s):** David A. Wallace and Margaret Hedstrom, 2009

**License:** Unless otherwise noted, this material is made available under the terms of the **Creative Commons Attribution Noncommercial Share Alike 3.0 License:**  
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

**We have reviewed this material** in accordance with U.S. Copyright Law **and have tried to maximize your ability to use, share, and adapt it.** The citation key on the following slide provides information about how you may share and adapt this material.

Copyright holders of content included in this material should contact [open.michigan@umich.edu](mailto:open.michigan@umich.edu) with any questions, corrections, or clarification regarding the use of content.

For more information about **how to cite** these materials visit <http://open.umich.edu/education/about/terms-of-use>.

# Citation Key

for more information see: <http://open.umich.edu/wiki/CitationPolicy>

## Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }



**Public Domain – Government:** Works that are produced by the U.S. Government. (USC 17 § 105)



**Public Domain – Expired:** Works that are no longer protected due to an expired copyright term.



**Public Domain – Self Dedicated:** Works that a copyright holder has dedicated to the public domain.



**Creative Commons – Zero Waiver**



**Creative Commons – Attribution License**



**Creative Commons – Attribution Share Alike License**



**Creative Commons – Attribution Noncommercial License**



**Creative Commons – Attribution Noncommercial Share Alike License**



**GNU – Free Documentation License**

## Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }



**Public Domain – Ineligible:** Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) \*laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }



**Fair Use:** Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) \*laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

# SI 655

## Management of Electronic Records

Week 7

March 9, 2009

Promoting Accountability:  
Compliance and Audit

# Outline

- *Assessing risk*
- *Measuring compliance*
- *Incentives for compliance*

# Risk

- Anything that prevents the organization from meeting its objectives
- Combination of the probability of an event (usually adverse) and the nature and severity of the event. (ERPANET, *Risk Communication Tool, 2003*, [www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf](http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf))

# Risk Assessment & Management

- identifying risks
- assessing magnitude and probability of occurrence
- deciding on an appropriate response (risk avoidance, acceptance, reduction...)

(Gable 2005)

# TABLE 1: CONSEQUENCES OF FAILING TO MANAGE RECORDS/INFORMATION RISKS (Lemieux, 2004)

| Sector(s)  | Primary Risk                            | Secondary Risk(s)  | Cause of Risk   | Consequence of Risk   |
|--|---|--|---|---|
| Investment Banking                                       | Legal <sup>2a</sup> and regulatory risk | Financial <sup>2b</sup> and reputational risks <sup>2c</sup> | Failure to preserve e-mail in accordance with Securities and Exchange Commission rules          | \$1.65 (U.S.) million fine each against five investment banks   |
| Auditing and Management Consulting (Arthur Andersen LLP) | Legal risk                              | Financial and reputational risks                             | Inappropriate destruction of records  | Found guilty of obstructing justice<br><br>Subsequent corporate failure   |
| Utilities (Transco)                                      | Operational risk <sup>2d</sup>          | Legal and reputational risk                                  | Lost regional records of the number of gas leaks left for repair                                | Engineers waste time and money as they are asked to work on pipes they cannot find<br><br>Health and safety executive investigation follows |
| Science and Technology (NASA)                            | Operational risk                        | Environmental risk <sup>2e</sup>                             | IT obsolescence leads to disappearance of valuable satellite records documenting global warming | Inability to track global warming with potential long-term environmental consequences that are, as yet, unknown                             |

# 2007: Sea change (2005: The tide is turning)

- **Retention**

- Inadequate programs (consideration; performance; record creating technologies; backups; responsibilities) irregularly followed; ignore ER

- **Litigation/Regulation**

- Increases in hold orders responsiveness but many ignore ER; difficulty complying w/ discovery requests

- **Preservation**

- Inadequate/absent migration plans; IS/IT unaware of eventual migrations

- **Life Cycle Management**

- Inadequate RM responsibility for ER; IS/IT unaware of "lifecycle"; heightened awareness over meeting litigation challenges; heightened belief in accuracy, reliability and trustworthiness over time

(Cohasset/AIIM/ARMA 2007)



# RM Self Assessment Tool

- "Are electronic records addressed in your organization's records management policies and procedures?"
- Are electronic records included in your organization's retention schedules?
- Does your organization's hold older system include electronic records
- Have funding and resource levels for records management in your organization kept pace with the tremendous growth in volume, types, and complexity of electronic records?
- Is there a forum for regular interaction between business units, records management, legal and compliance, and IS/IT to collaborate and cooperate on recordkeeping requirements and initiatives?
- Are business units and individuals held accountable for compliance with records management policies and procedures?
- Does your organization have a plan and budget to migrate digital records that need to be preserved for more than 7 years or preserved permanently?"

# Approaches to Risk Assessment

- Institutional level
  - Mission critical systems
- Functional level
  - Business systems
- Administrative systems
  - records management, security, inventory control, etc.
- Records management
  - mission critical systems with high impact / high probability of risk

# Risk Probability Scale

| LABEL     | VALUE | DESCRIPTION                            |
|-----------|-------|--|
| Very High | 5     | A probability estimated between 26–99% |
| High      | 4     | A probability estimated between 11–25% |
| Moderate  | 3     | A probability estimated between 6–10%  |
| Low       | 2     | A probability estimated between 1–5%   |
| Very Low  | 1     | A probability estimated below 1%       |

© PD-INEL

Appendix A: *Risk Management of Digital Information* (CLIR, 2000) [www.clir.org/pubs/reports/pub93/contents.html](http://www.clir.org/pubs/reports/pub93/contents.html)

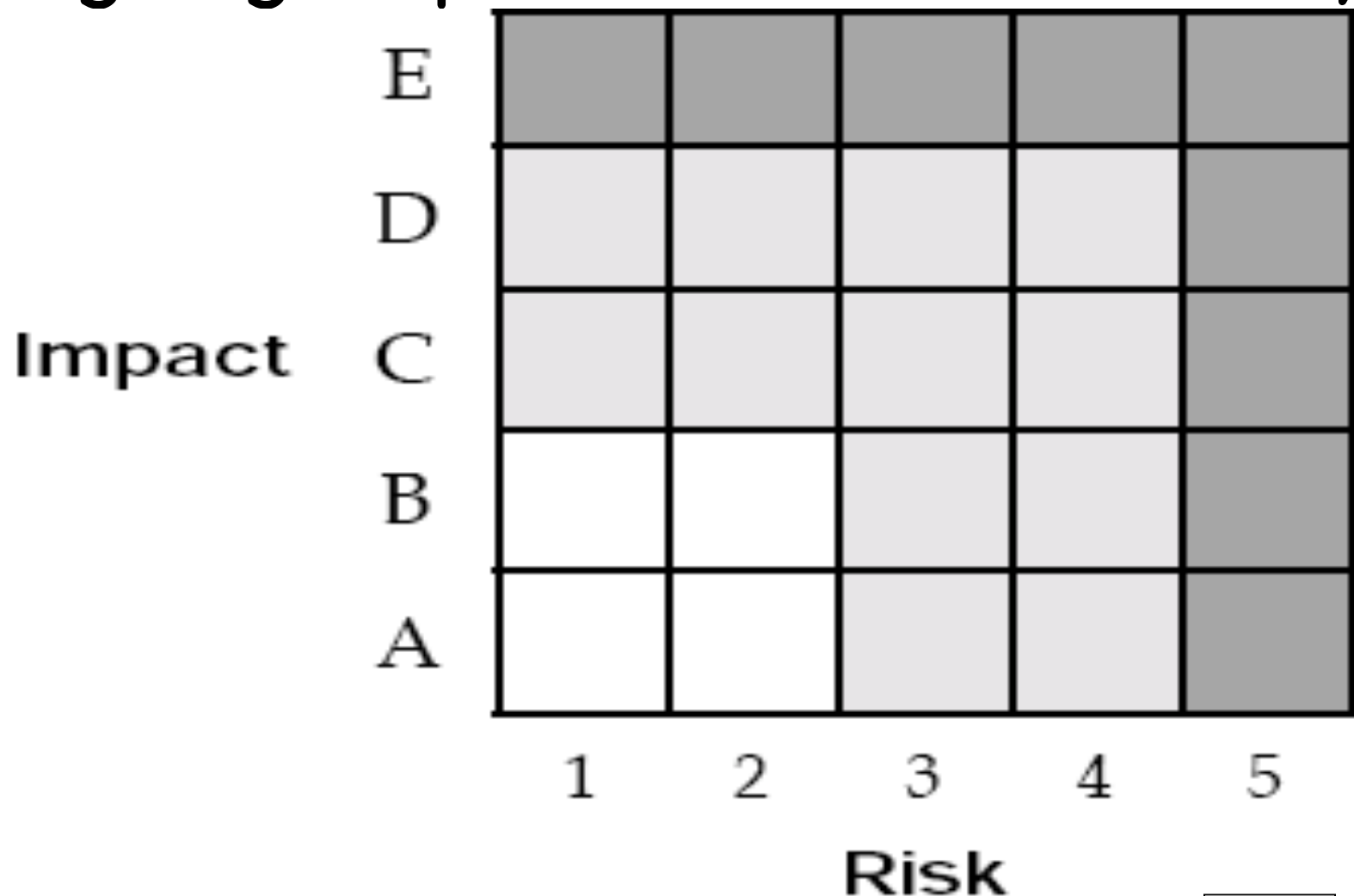
# Risk Impact Scale

| LABEL        | VALUE | DESCRIPTION   |
|--------------|-------|---|
| Catastrophic | E     | Complete, irreversible loss of data. Data cannot be drawn from other sources—print, artifact, or digital. |
| Very Serious | D     | Partial, irreversible loss of data. Data cannot be drawn from other sources.                              |
| Serious      | C     | Complete loss of data. Data can be fully reconstructed from other sources.                                |
| Significant  | B     | Partial loss of data. Data can be fully reconstructed from other sources.                                 |
| Minor        | A     | Complete or partial loss of data. Data can be copied from other data files.                               |

© PD-INEL

Appendix A: *Risk Management of Digital Information* (CLIR, 2000)

# Aligning Impact & Risk Probability



© PD-INEL

Appendix A: *Risk Management of Digital Information* (CLIR, 2000)

## Qualitative Severity Scale Matrix

| Effect \ Likelihood                                     | Unlikely            | Seldom              | Occasional          | Likely              | Frequent            |
|---|---------------------|---------------------|---------------------|---------------------|---------------------|
| Loss of Asset<br>(catastrophic event)                   | Extremely High Risk | Extremely High Risk | Extremely High Risk | Extremely High Risk | Extremely High Risk |
| Loss of Function/operational<br>ability)                | High Risk           | High Risk           | High Risk           | High Risk           | Extremely High Risk |
| Loss of capacity with<br>compromise of some<br>function | Moderate Risk       | Moderate Risk       | Moderate Risk       | High Risk           | Extremely High Risk |
| Loss of some capability with<br>no effect on function   | Low Risk            | Low Risk            | Moderate Risk       | Moderate Risk       | High Risk           |
| Minor or no effect                                      | Low Risk            | Low Risk            | Low Risk            | Low Risk            | Moderate Risk       |



© PD-INEL

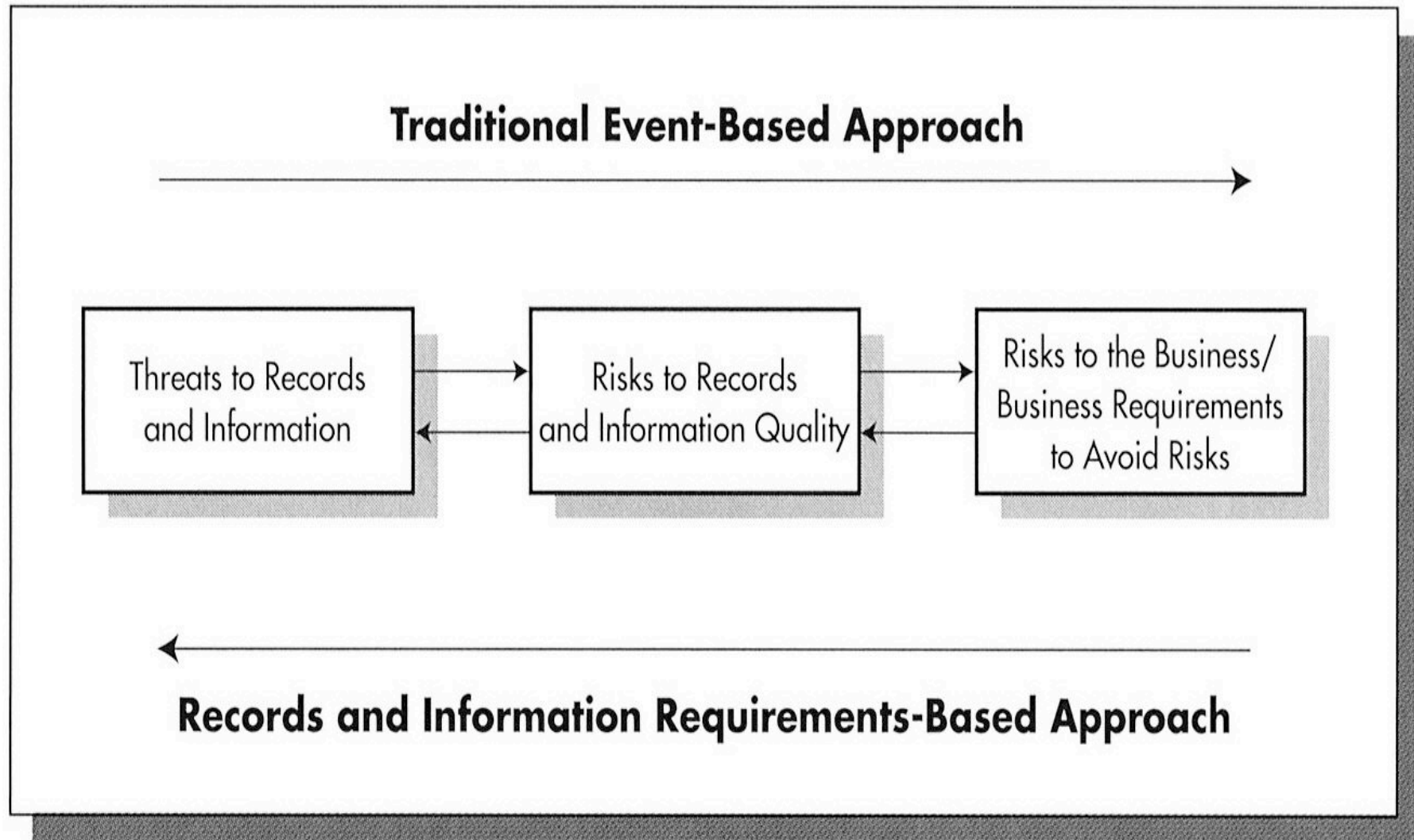
ERPANET, Risk Communication Tool (2003) [/www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf](http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf)

## “Table 2 Event-based Records and Information Risks

### Trigger Event

- Disaster - Natural or Human caused (e.g. fire, flood, earthquake)
- Major system outages or disruptions caused by system or human errors
- Computer fraud
- Theft of electronic information and electronic information assets
- Theft of computer system resources (e.g. use of organization's computer systems for other than official purposes)
- Malicious attacks and harmful code (e.g. virus attacks, hackers, etc.)
- Unauthorized disclosure of electronic information
- Errors and omissions in documentation
- Inadequate retention periods for records and information”

**FIGURE 1 Approaches to Identifying and Managing Records and Information Risks**





# Risk management

- a process of managing inherent risk
  - Identifying potential risk and impact on organization
  - Identifying controls that reduce risk
  - Assessing the qualities of controls
- Objective – reduce risk to manageable level
- Case Study: UM Risk Management Office

# Control structure

- Reduces risk because reduces the probabilities of errors
- Control includes an organization's:
  - resources
  - culture
  - processes
  - policies and procedures

# Compliance

- Compliance generally consists of three activities:
  - persuasion
  - monitoring
  - enforcement (Archives New Zealand 2001)
- Performance of policies, procedures, RK, technologies, training, audit
- RM outcomes?: more automated record declaration, classification; retention (Gable 2005)

# Persuasion

- Aims to promote the adoption of the required actions through ensuring that their purpose is understood.
- Should provide the motivation to perform. (Archives New Zealand 2001)
- RM strategies:
  - Law & regulation
  - Best practices & standards
  - Case law
  - Public meltdowns
  - Education & Training

# Compliance – monitoring

- Auditing
  - Planning
  - Evaluating the control environment – effectiveness and efficiency of policies and procedures
  - Conducting tests for compliance with policies, standards etc.
  - Writing report with recommendations for overcoming problems
- RM Strategies
  - Planning & Evaluation
  - Policy & Procedure compliance testing
  - Mitigation via records declaration, repository, classification schemes; retention, destruction, archiving...

# Compliance Tools

- Performance Reporting
- Incident Reports (failures that lead to remedies)
- Self-Assessment
- External Audits
- Inspections

# Compliance Surveys

- Common pitfalls evidenced:
  - Focus on technological deficiencies
  - Ignore gaps in
    - Practice
    - Standards
    - Documentation
    - Oversight
    - Assigned Responsibility
    - Accountability

(Gable 2005)

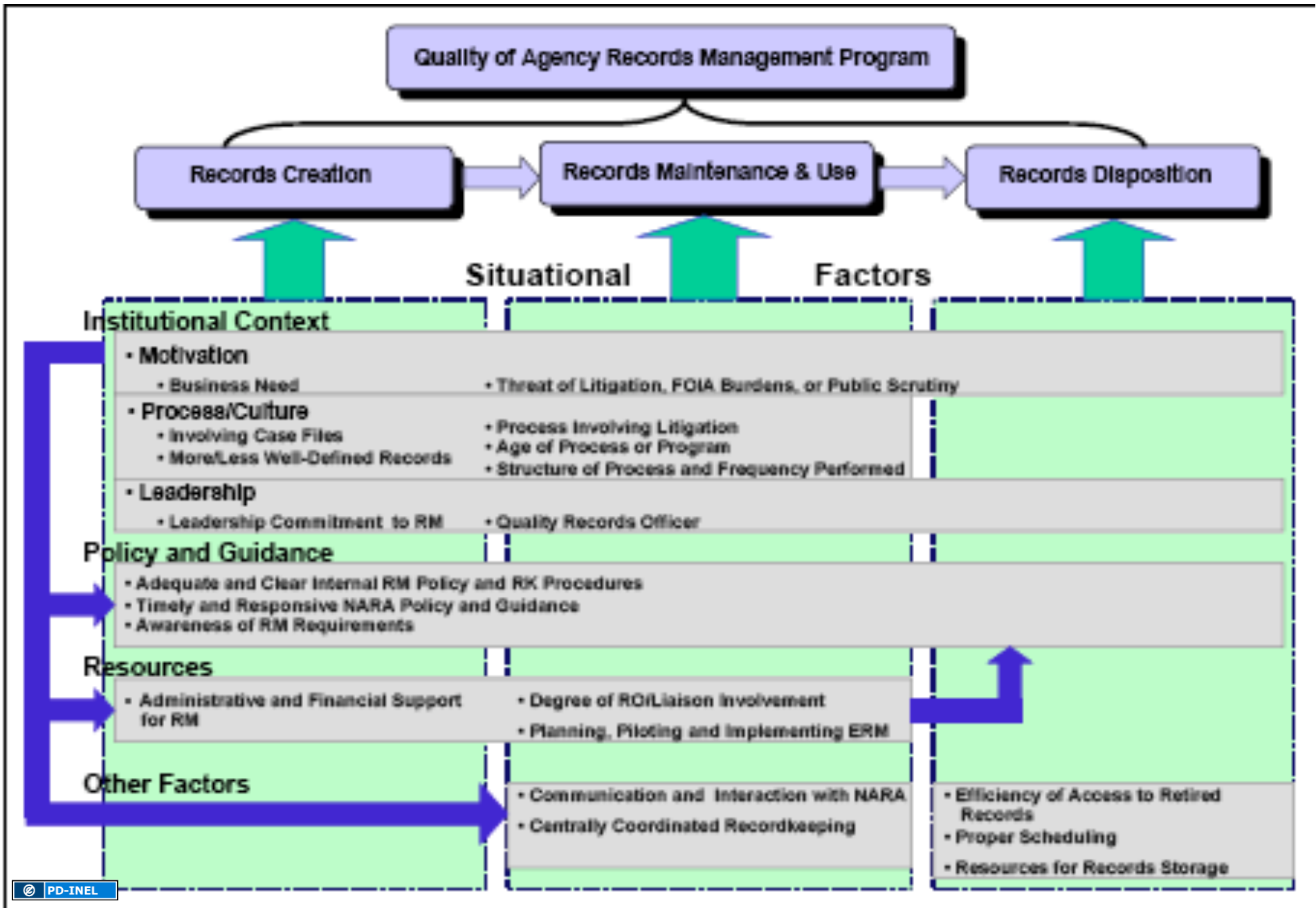
# Drivers for RM Compliance

## NARA/SRA Survey (2001)

- Institutional Context
  - Motivation (Business Need, Threat of litigation, FOIA Requests, Public Scrutiny)
  - Process/Culture (well structured records, maturity, age, consistent use)
  - Leadership
- Policy and Guidance
- Resources
- Other Factors
  - frequency of communication with RM; centralization / decentralization; scheduling and storage



# NARA/SRA STUDY: SITUATIONAL FACTORS MODEL



# Conclusion

- One size does not fit all
- Alignment of risk and compliance
- Knowledge of specific requirements
- Need for ongoing monitoring and improvements