Risk Management: Simple and Relevant
or *how do I get there from here?*

Risk Management and Global Standards Workshop
Ottawa, April 20, 2007

John Shortreed
Director, Institute for Risk Research
University of Waterloo
Canadian Expert to ISO 31000
shortreed@uwaterloo.ca,

Objectives for next hour

1. Map your present risk management framework & process onto ISO 31000
2. What ISO 31000 is anyway? – *having seen how it can be used for applications (audit) and where it came from (history)*
3. Ask questions – *please interrupt, this is a workshop*
4. Implementing ISO 31000? *Motivations for and suggestions for changing your framework/process*

My 25 year history in risk management & *Lessons Learned*

- 1980 Transport of Hazardous Materials - *cause and effect understanding of risk – became de facto world standard*
- Safety of the Canadian Blood System today (Krever) - *every level in organization must have **the same** risk conceptual reality*
- 8 years local politician – *decision making is different*
- Risk Costs Benefits of Therapeutic Drugs- *need to work with stakeholders (especially doctors) to achieve meaningful change*
- Safety of Software – *sometimes only limited understanding*
- Xenotransplantation? - *communication and consultation*
- ISO terms (2002), standard 31000 (2009) - *the future of risk management*
- 2006 –Gold standard is bhpBilliton – *yield 2 min*. to *Grant*
- Navigation safety – *integrating expert opinion and data*
- *2007 – How to deal with & explain positive and negative risk?*

ISO 31000 a risk management standard/guide

- ISO 31000 like any standard is a

common vision of shared concepts

of risk, and risk management

- Over the back fence test – talk to your neighbor, *who is in entertainment*, about what works in risk management?

Illustration – Dryden Air crash (28 dead – inquiry – wing icing)

- One of 100+ recommendations was to have joint NA research into risk –> workshop in Montreal
- 3 days with 50 top international people - a total waste of time (except to check off #128 as done!)
- Everyone had a different framework from Vern Gross to CSA Q850 (also at different levels)
- Everyone had different terminology
- Have you had similar experiences?

Basic 31000 Building Blocks

(a work in progress but more or less there now or by the end of next week)

Thousands of existing standards (modified?) and new risk standards

Medical devices ISO standard (also Canada)

Internal Audit Standard COSO (revised)

Pet food HACCP (ISO?)

etc. etc. etc.

CSA Q850(1997) revised

Any manager anywhere deciding anything

Risk Management **Process** – Clause 6

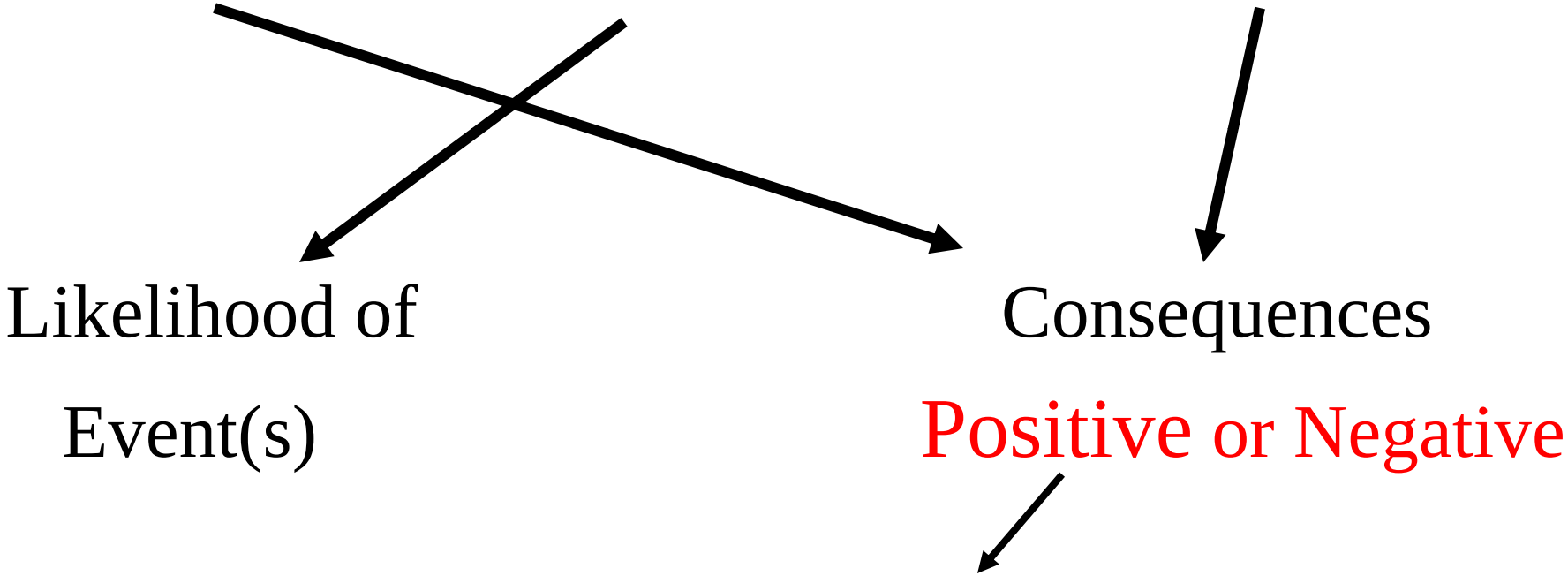
Organization-wide **Framework** – Clause 5

Principles (Clause 4 and Annex A and B)

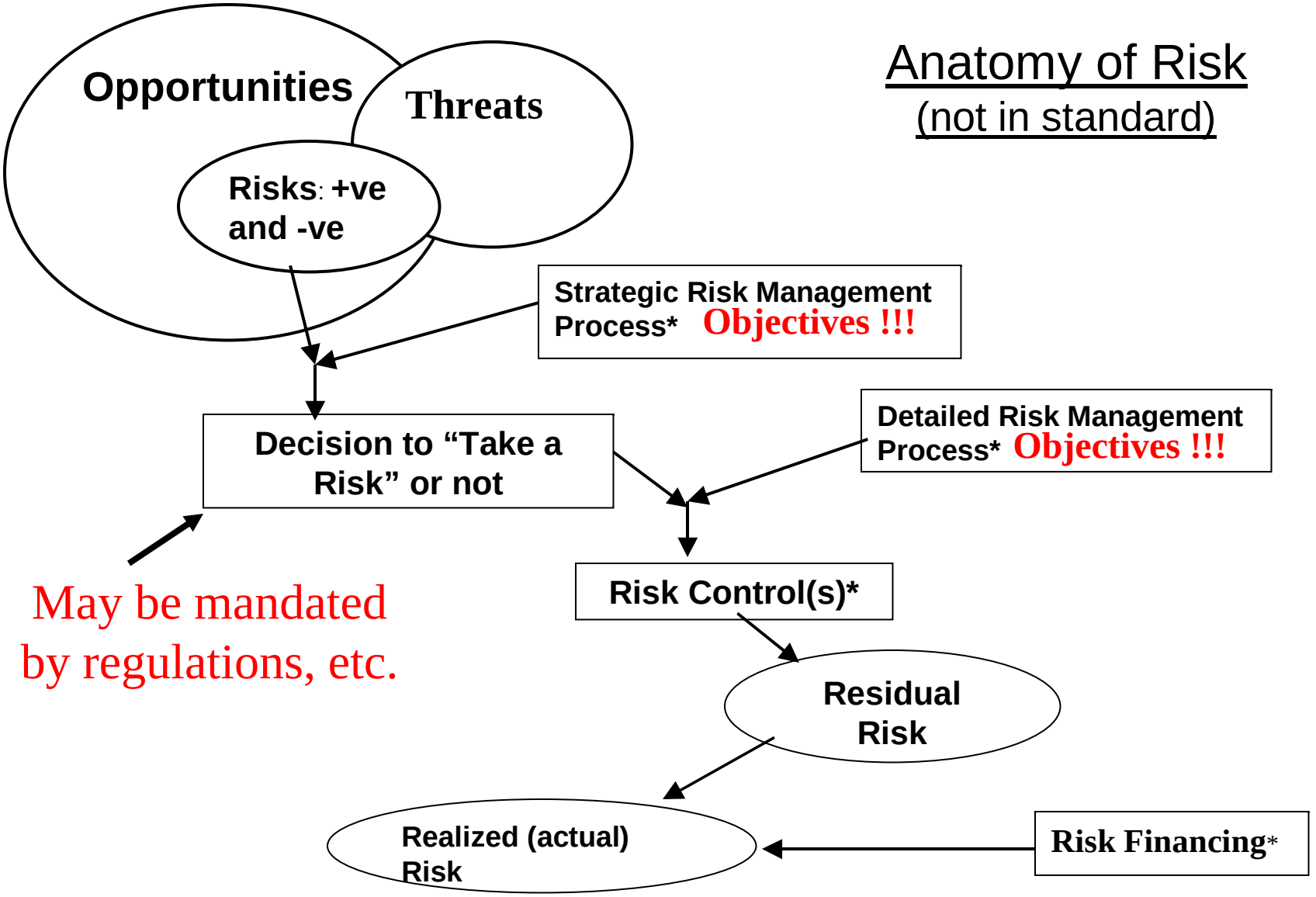
Definitions –ISO Guide 73 (2002 revised) – *handout is CA proposal*

Risk is

"Effect of Uncertainty on objectives"



Anatomy of Risk
(not in standard)



Positive and Negative Risk ??? Look to Objectives, good ↑ or ↓ always some of each

examples

Huge risk management success story of last 20 years → ***control of inflation by interest rates plus communication & consultation*** – economy up uncertainty down

Regulation of *"your product"* want safety for public (reduce neg. risk) and also growth of economy&benefit through stable, level, well known playing field (increase pos. risk) [planes, ships, medical equip]

Framework & Principles for ERM is a major emphasis of ISO 31000 – organization-wide

- Principles given; evidence based, structured, uncertainty explicit; tailored, transparent, dynamic, part of decision-making, add value
- Based on continuous improvement
- Requires links to strategic planning, governance, accountability, commitment, monitoring, communication and consultation
- Not intended for certification but can use for self assessment

“A decision that doesn’t involve risk probably isn’t a decision” - Peter Drucker

- How can a risk management department possibly assist every manager with every decision?

- good to reduce negative risk, why not increase positive risk?
  - focus groups to find out what works
  - partnerships to ensure success (FedX and Kinkos)
  - bonus innovation, performance

- Manager’s risk performance is part of overall evaluation

ISO 31000 on integration of Risk Management

"contrast to common practice"

- All key risk management processes are not "stand alone" but integrated into main activities and processes of the organization – every manager is a risk manager
- Risk management is always viewed as a core process, risks are considered in terms of sources of uncertainty that can be treated to maximize the chance of gain while minimizing the chance of loss.
- Regarded by senior managers as essential for the achievement of objectives
- Governance structure founded on risk management
- What changes would your organization have to make?

Example PRINCIPLES OF MANAGING RISKS TO THE PUBLIC –UK Cabinet Office (2004?)

- **Government will be *open and transparent* about its understanding of the nature of risks to the public and about the process it is following in handling them**
- **Government will seek wide *involvement of those concerned* in the decision process**
- **Government will act *proportionately and consistently* in dealing with risks to the public**
- **Government will seek to base decisions on all relevant *evidence***
- **Government will seek to *allocate responsibility* for managing risks to those best placed to control them**

Integrate your Risk Management into 31000 requirements (clause 5)

- Required to have every manager
  - do their **own** risk management and controls,
  - know what risks they **own**,
  - prepare their **own** reports,
  - do their **own** communication
  - Do their **own** monitoring
  - Be **rewarded** for doing risk management

Integration (verb), not embed or aligned

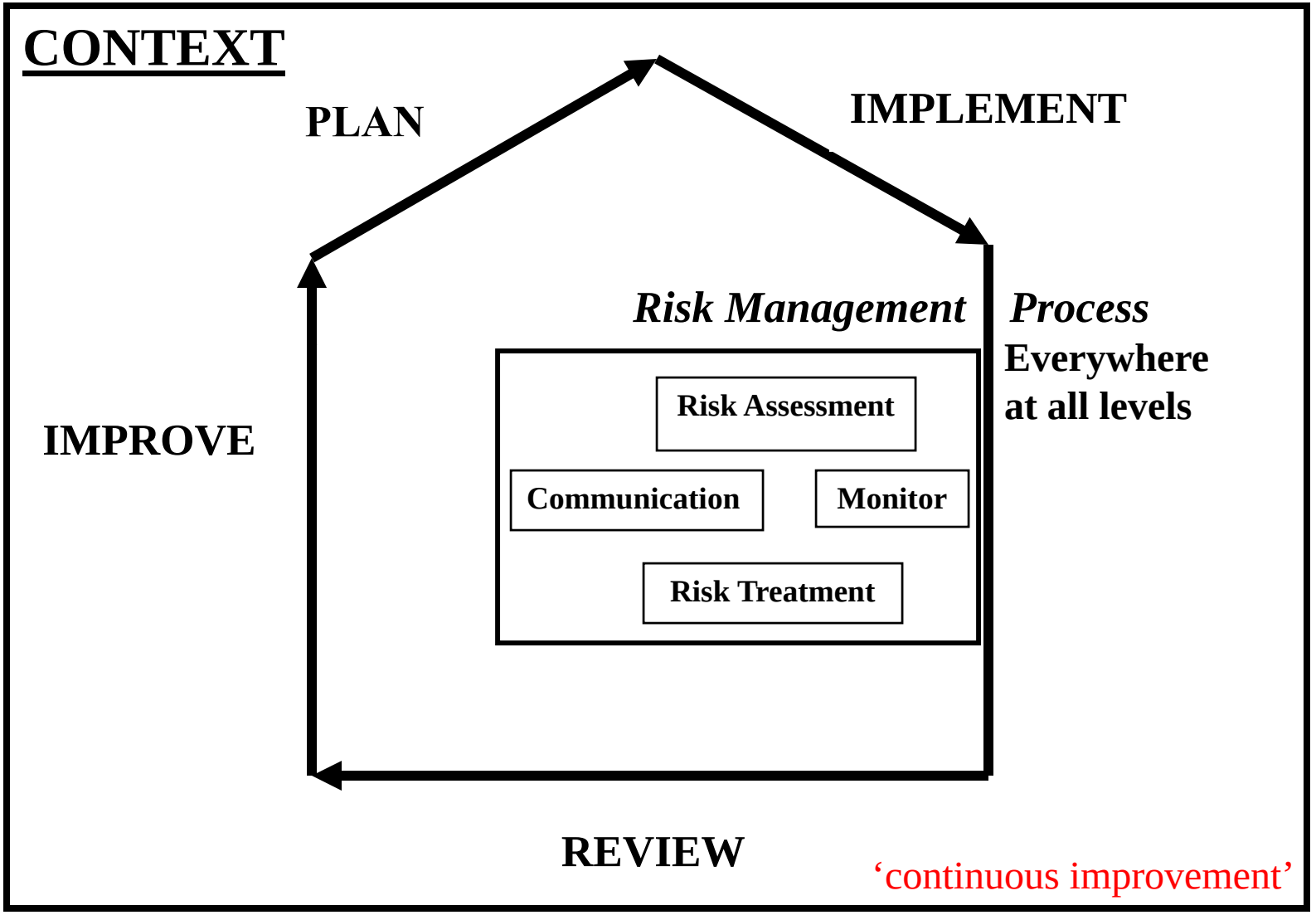
Key difference; ISO means integrate, many embed or even *the dreaded* "add on" – ISO will say ???

- To make whole or complete by adding or bringing together parts – Webster, 2nd
- To bring (parts) together into a whole; to unify – Webster, 2nd

- Embed – to set or fix firmly in the surrounding mass; as, the knife was *embedded* in the wood

Framework for Integrating Risk Management Organization-Wide

31000 requires on ERM "Framework" (this is one proposal for ISO)

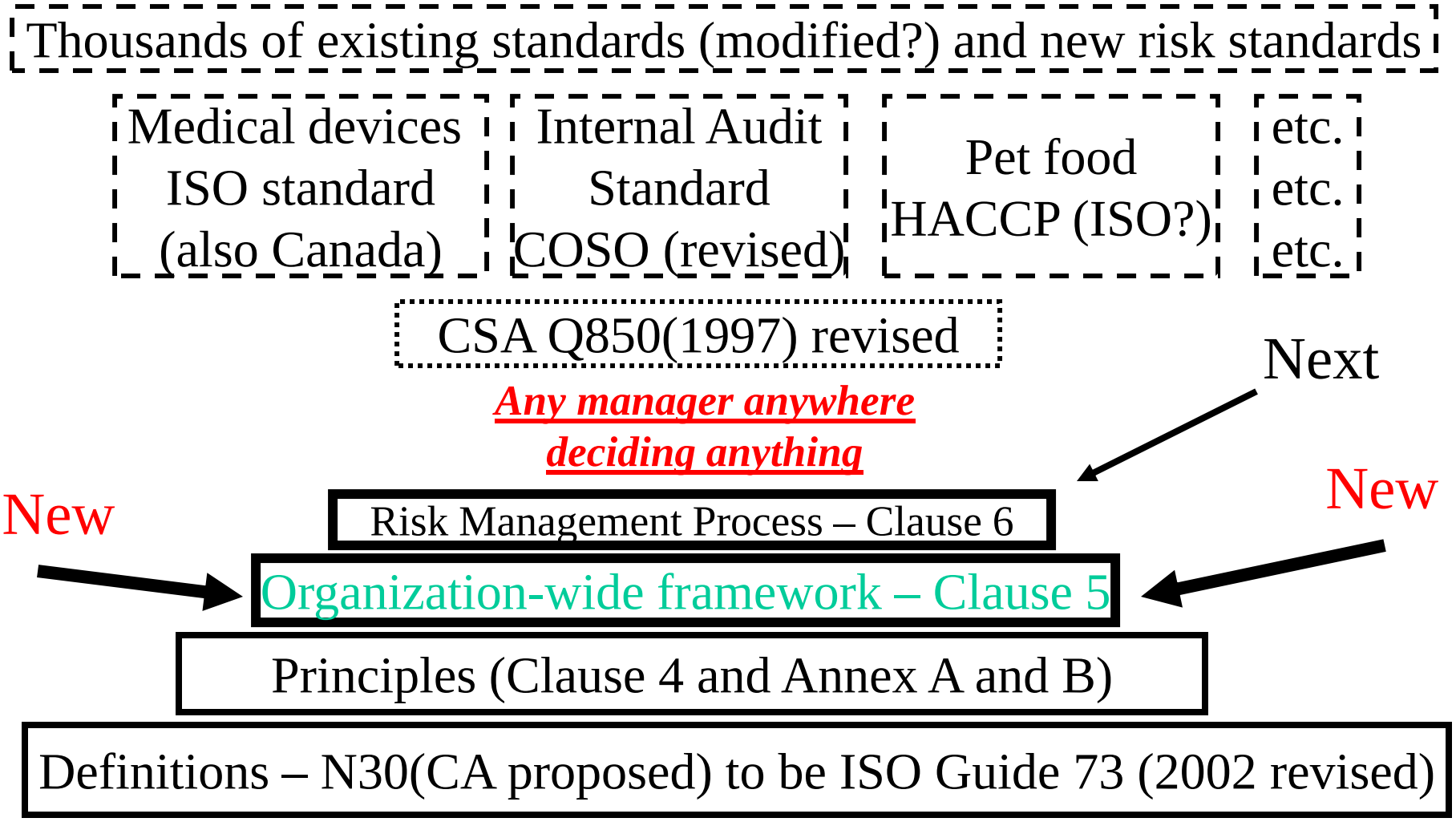


Example – Framework Mapping (Treasury Board, 2004?)

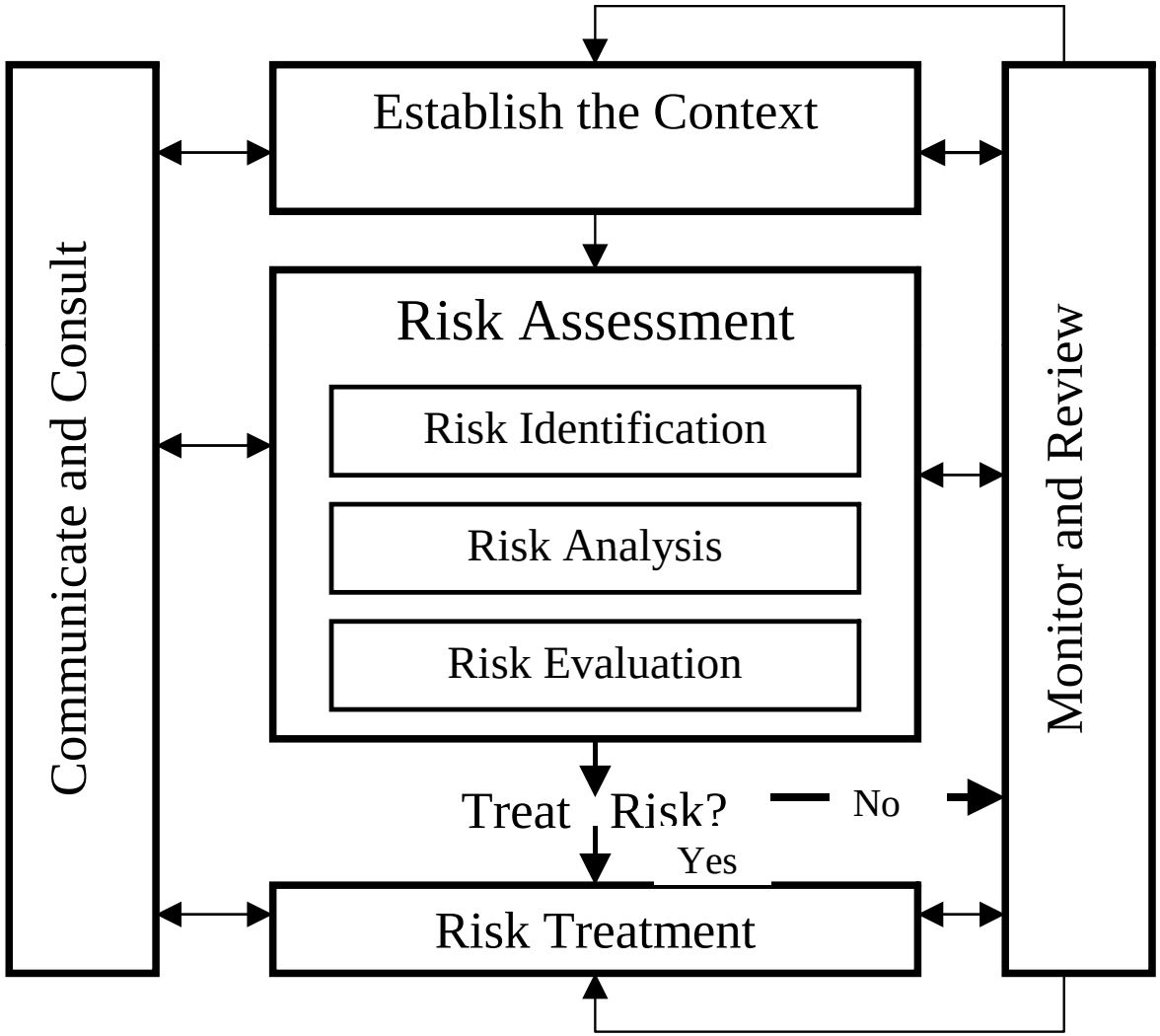
- Develop corporate risk profile
- Once corporate risks are know and the infrastructure has been identified and mobilized, the key actions for practising integrated risk management are to:
  - Engage the whole organization
  - Enable people with tools and techniques
  - Sustain a supportive culture and processes
  - Consult and communicate throughout the process
- Use common risk management process
- Continuous risk management framework and process improvement

Basic 31000 Building Blocks

(a work in progress but more or less there now or by the end of next week)



Risk Management Process
Understanding = Risk assessment



strategic to operations – ISO requires same *generic* risk management process

- Conceptual reality and process all the same, *tools*, *techniques*, *reporting*, *communications differ* but context, risk appetite, risk criteria the same
- Any manager can audit any other manager; huge opportunity for training and continuous improvement
- Incorporation of existing well developed risk management encouraged; e.g. clinical studies, standard operating procedures, software comprehension
- Expect in time existing methods will modify terms, align processes to be conceptually identical

Example of top to bottom integration
Safety of blood system today? (Krever)

- How to rate overall safety with 6th generation detailed international audits for day to day operations ?
- What about costs, product assurance, quality control, process design, cost optimization, not to mention 17 different Canadian centers!
- What about Life Saving Benefits of blood?
- Adjusted FDA's 'current good manufacturing process' to incorporate "conceptual" vertical integration
- Used "continuous improvement" framework for evaluation – audited against ideal 'ERM' system with special emphasis on what happened when there were deficiencies
- Successfully used in unique audit to support recommendations

Key elements of RM Process - risk understanding

(aka risk identification, analysis, and a little bit of evaluation)

- Focus on understanding since main purpose is to assist decision-maker, not produce numbers –but #'s are gold standard (navigation example)
- Evidence of cause and effect – search out reversal of cause, contrary indicators, frequent mistakes, discontinuities, analogies, longitudinal and cross section studies, human factors, expert opinion
- Stakeholders are key – decision data, consultation, impact on decisions, (Brent Spar example)

Example – **Risk Analysis** for Marine Navigation Policy – "cut 25% of Aids"

- Data is inadequate, how to use it with expert opinion and obtain credible results
- Build "physical" models, calibrate to
  - Pilots
  - Captains of Coast Guard vessels
  - Meso level data for 23 years in St Lawrence
- *Worked but must leave time for "buy in"*

Example Communications – Brent Spar

- Shell plans the right thing - to sink obsolete equipment at sea.
- Story “leaks out” and reputation gets hammered in press,
- Shell changes to the wrong decision ‘take to shore and cut up”
- Later even GreenPeace said they were wrong and Shell was right in the first place
- If all risks had been involved with the decision from the outset including reputation risk, not just environmental risk then the views of stakeholders would have been front and center with lots of risk communication & consultation with Public
- Likely right decision with big $ and reputation payoffs

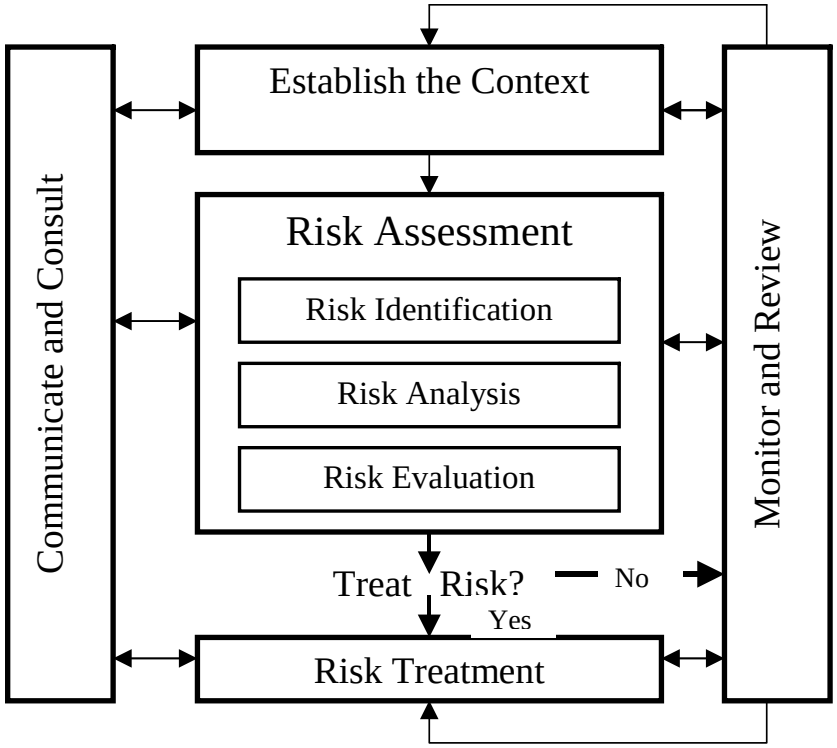
Example: link Process to objectives Mayo Clinic

Continuous Improvement to be #1

- Mayo's objective is to be #1, they have:
  - Lots of money
  - Team approach from beginning
  - Continuous improvement approach
- Method is SOP, Standard Operating Procedure, only one way to do any procedure/operation
- Collect data on outcomes, review and modify SOP to maintain #1

ISO 31000 Risk Management Process

Consider the obvious – how much improvement is possible with only one process with only one graphic with only one set of concepts and definitions – some Canadian examples follow to illustrate the obvious



Mapping Existing RM Process & Framework To 31000 – Example 1

Risk Identification

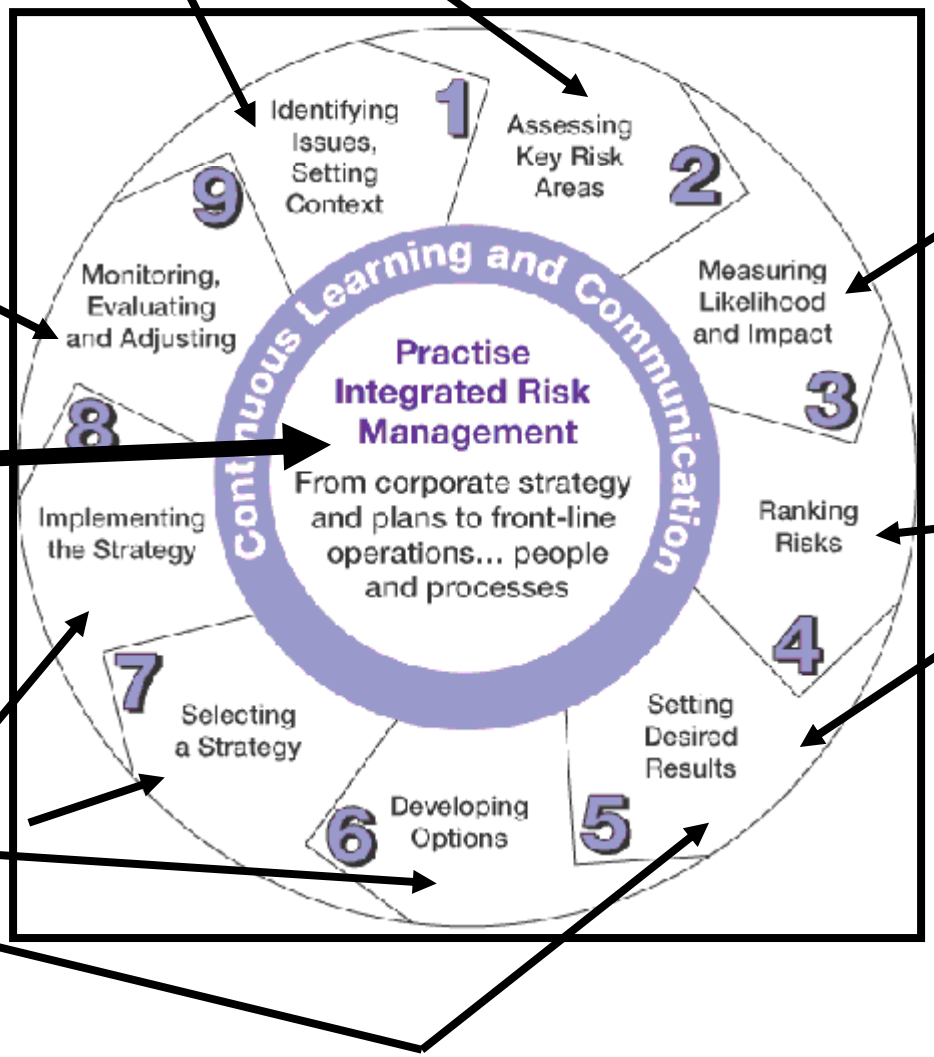
Risk Analysis

Risk Evalution

Monitoring & Review

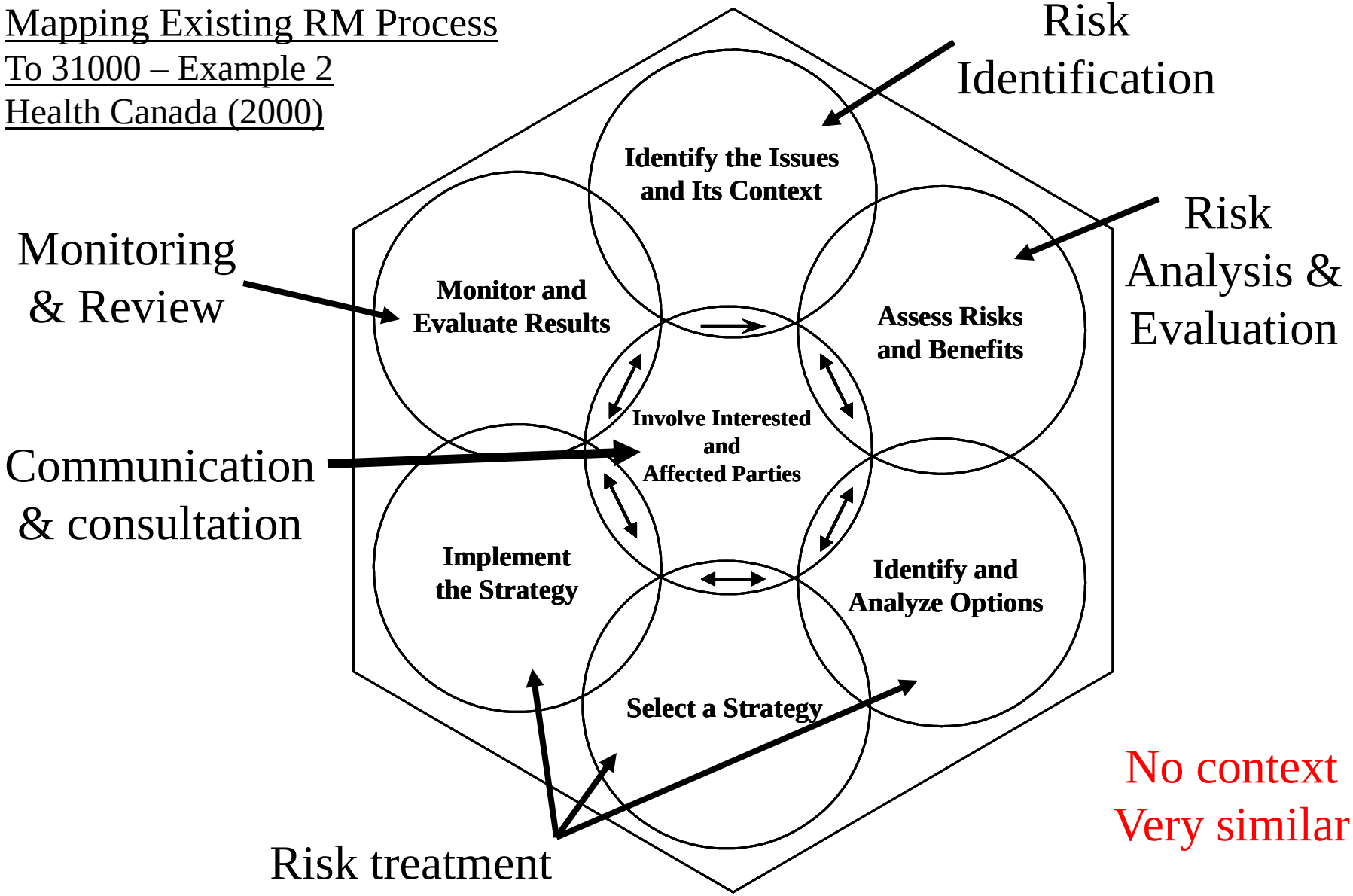
Organization-wide Risk Management Framework and communications

Risk treatment



Other
-context?
-risk is neg?
-risk ownership?

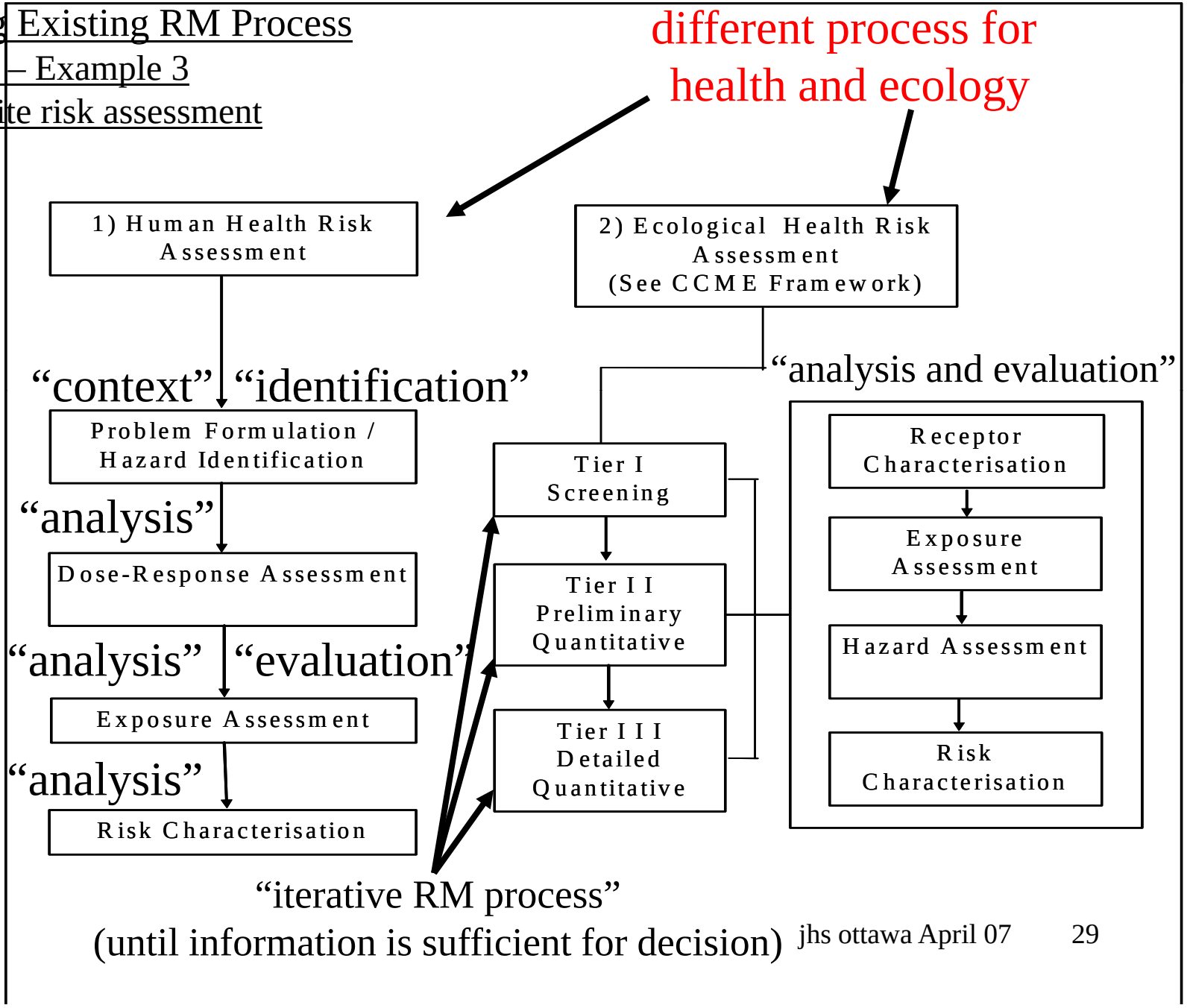
Mapping Existing RM Process
To 31000 – Example 2
Health Canada (2000)

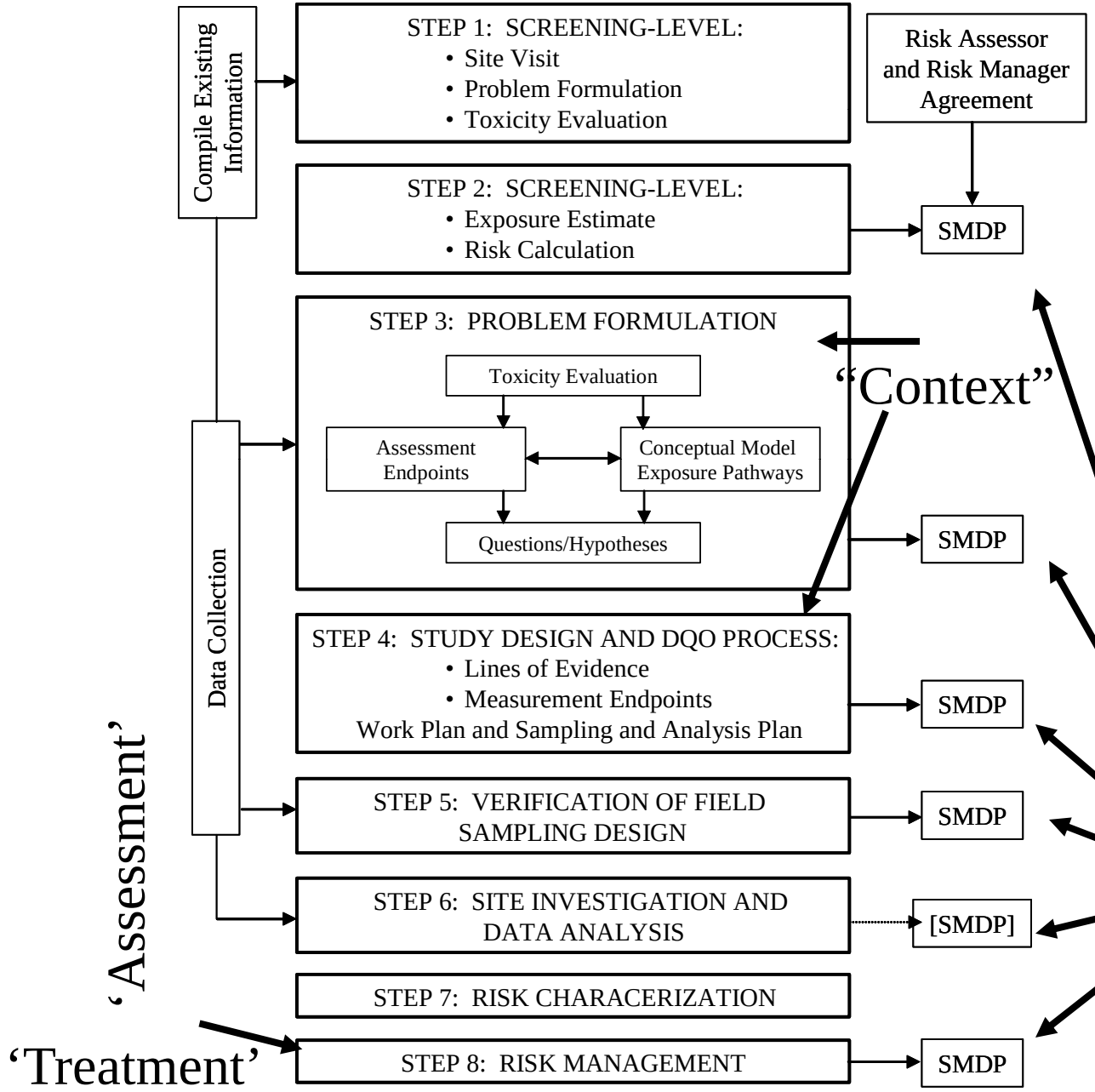


No context
Very similar

Figure B-2. Health Canada Decision-Making Framework for Identifying, Assessing and Managing Health Risks (2000)

Mapping Existing RM Process To 31000 – Example 3 Ontario site risk assessment

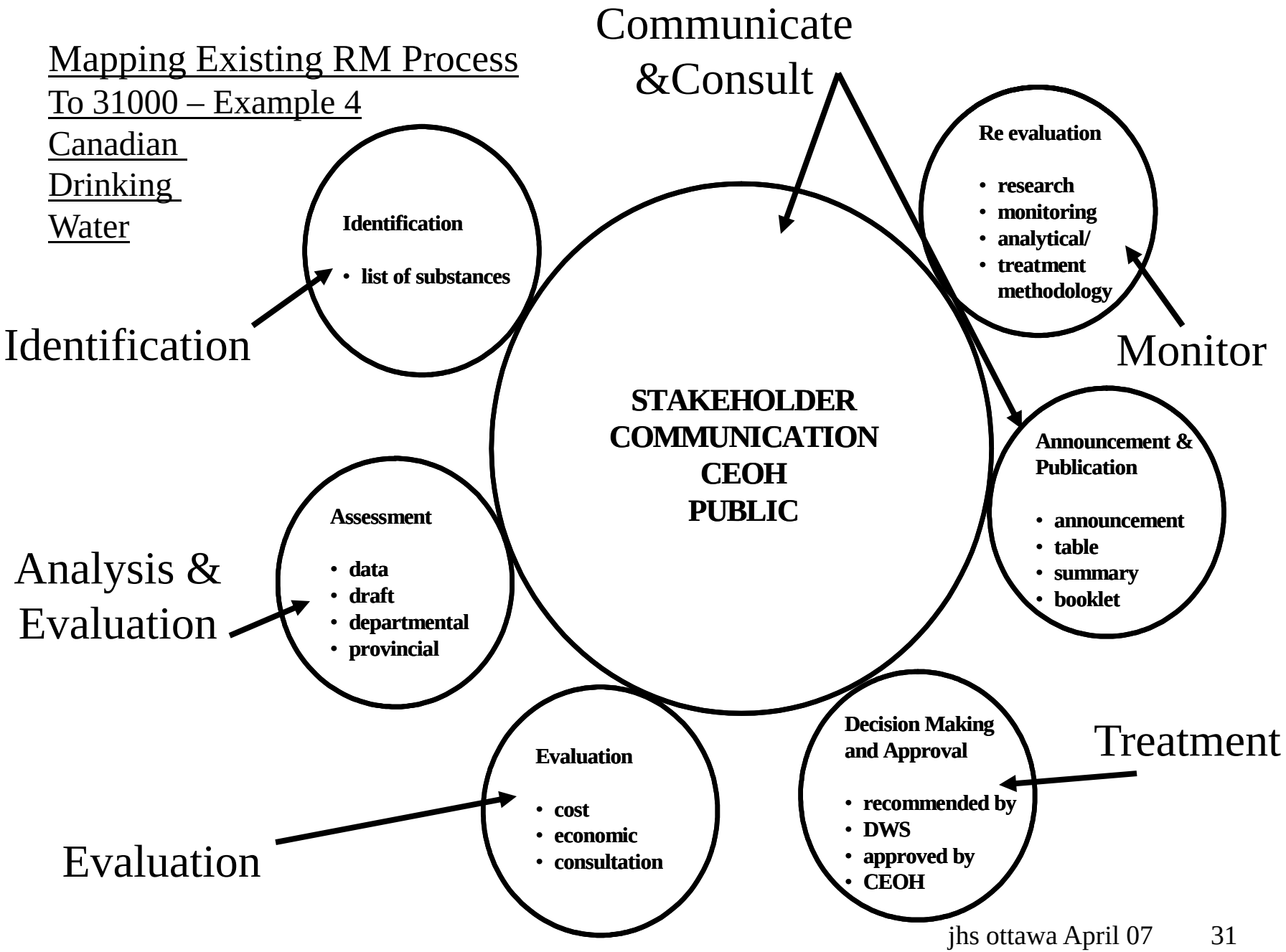




RAGS
-Iterative (2x)
-Context given

SMDP - Scientific/Management Decision Points

Mapping Existing RM Process To 31000 – Example 4 Canadian Drinking Water



MANAGEMENT TASK	FUNCTIONS[3]	CRITERIA	CAPACITY REQUIREMENTS
SENIOR MANAGEMENT **"STRATEGIC"**	• Decision-making • Monitoring • Stakeholder Relations • Context	• Agency Objectives • Capacity • Trust of Stakeholders • Transparency • Flexible-Consistency • Budget	• Risk Communication and Consultation • Documentation • Best "Practical" Practice • Partners • Staff
POLICY & PROGRAM PLANNING **"TACTICAL"**	•Preliminary Analysis (Identification) • Risk Analysis • Risk Treatment Options • Evaluate Risk and Risk Treatments	• Cost-Effective • Stakeholder Acceptance • Uncertainty Explicit • Reasonable Relationship • Precautionary Principle • Comprehensive	
OPERATIONS **"OPERATIONAL"**	• Implement • Quality Control • Programs to Reduce Risk	• Achieve Operational Plan • Correct Failures • Continuous Improvement • Customer Satisfaction	

Eac cap app all fun lev

Example from IRR (2001) – again no common basis for understanding is evident even though interesting

Wish there was more time for

- Risk management is risk business – can be 100% wrong - key role for
  - *communication and consultation*
  - *'review, review, and review'*
- Human factors for risk controls
  - Nick Leeson and Brian Hunter (Canadian is #1)
  - John Arnold + 2 billion $US last year; that's +ve
  - aircraft crash in BC; clash of economics and safety
  - HSE >5 people in workplace failure
- Software and other special cases

Summary- did we meet objectives?

- What ISO 31000 is anyway?
- Map your present risk management framework & process onto ISO 31000?
- Your questions answered – *please interrupt– this is a workshop –* --- */ 10*
- Implementing ISO 31000? *Suggestions for risk management – no this is for the weekend*

Basic 31000 Building Blocks

(a work in progress but more or less there now or by the end of next week)

Thousands of existing standards (modified?) and new risk standards

Medical devices ISO standard (also Canada)

Internal Audit Standard COSO (revised)

Pet food HACCP (ISO?)

etc. etc. etc.

CSA Q850(1997) revised

Any manager anywhere deciding anything

Risk Management Process – Clause 6

Organization-wide framework – Clause 5

Principles (Clause 4 and Annex A and B)

Definitions –ISO Guide 73 (2002 revised) (CA proposed)

Framework for Integrating Risk Management Organization-Wide

31000 requires on ERM "Framework" (this is one proposal for ISO)