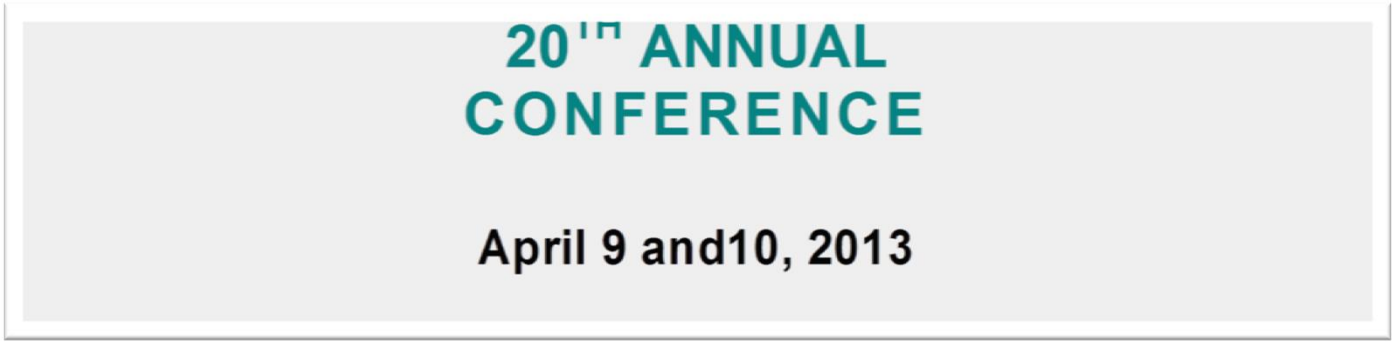
Auditing Association of Canada
L'Association canadienne de vérification

Colloquium



20TH ANNUAL
CONFERENCE

April 9 and10, 2013

Colloquium Questions

Guiding Questions for the Session

1. Can an existing EMS e.g. ISO 14001 or an H&SMS e.g. OHSAS 18001 be used as a risk management tool?

2. Does an existing MS align with other tools such as those used in an ERM?

3. Should the existing EMS or HSMS restrict its scope to environmental or H&S management? Reciprocally, how would an existing EMS or HSMS scope fit with a new ERM? Either way, what could be the issues to be addressed?

4. Should the existing EMS or HSMS seek opportunities to link with other management systems? If so, are there elements of the existing MS that can be used universally i.e. by all the MSs or the integrated MS? Are there some elements that should be unique or exclusive to the existing MS and some to the integrated MS? Does the term "integrated management system" appropriately describe an ERM?

5. Are the individual approaches or systems to manage a range of corporate risks consistent and should, or can, they be unified?

6. How would an internal audit program established for an EMS/EH&SMS have to be modified to address and ERM? The internal audit program including scheduling, locations, auditor qualifications/knowledge, workload, etc., etc., etc.

1. Can an existing EMS e.g. ISO 14001 or an H&SMS eg. OHSAS 18001 be used as a risk management tool?

Yes. Mgmt Systems can be integrated to have a single MS approach - ease & degree varies by organizations; can be staged evolution.

- A lot of similarities between MS and ERM – e.g. evaluation of aspects is risk based

- Gov - controls , R & R are common

Difference - ERM may not be sufficiently robust to manage specific EH&S risk

- could be effective tool depending on maturity of MS & assoc goverance

- must not be too audit driven / prescriptive

2. Does an existing MS align with other tools such as those used in an ERM

Alignment of MS with tools used in ERM

- Yes they could and should eg. aspects

- ERM may be to high level (macro) and lose actionable detail (eg. aspects micro level)

- Risk Ranking / registry may be similar, however may have unique aspects eg. 14001 / 18001 ranking or regulatory requirements rank may be unique.

* principles common

- Potential conflict of interest depending on reporting relationships

- Potential for EHS to be overshadowed by other enterprise risk - need to be aware of this risk and ensure no critical gaps.

- use familiar language (common) when implementing

3. Should the existing EMS or HSMS restrict its scope to environmental or H&S management? Reciprocally, how would an existing EMS or HSMS scope fit with a new ERM? Either way, what could be the issues to be addressed?

- Scope
  - Generally should restrict scope, but identify overlap.
  - Need to identify issues that are truly enterprise wide & communication to/make key players / stakeholders aware
- Depends on size of organization, & maturity of Mgmt System, & Business Planning strategy
  - Opportunity to merge should be explored - potential efficiencies
  - Can work and potential issues are manageable
  - Depends on nature and size of organizations - may need to align with organizations focus areas. (degree varies with organizations priorities)
  - Issue include:
    - Granularity variable
    - Align risk models & terminology and integration to ensure consistency,
  - Ensure common language to varied audiences

4. Should the existing EMS or HSMS seek opportunities to link with other management systems? If so, are there elements of the existing MS that can be used universally i.e. by all the MSs or the integrated MS? Are there some elements that should be unique or exclusive to the existing MS and some to the integrated MS? Does the term “integrated management system” appropriately describe an ERM?

- ``link vs. Integrate`` * recognise distinction between linkage and integration

  - Yes, you can link, shared / common procedures, e.g training and documentation .

However – some things such as policy and objectives, targets and programs should remain separate, limits competing interests.

- results in becoming part of normal conduct of business - not multiple hats
- potential to reduce audit fatigue
- ERM may be to high level & lose important risks at MS levels

Yes, but not optimal - universal elements

- unique requirements may need a unique approach - most elements can be universal

Integration of ERM:

- driven by the scope of EMS
- to what extent / depth should ERM be integrated?
- need conceptual process + sufficient detail to implement.
- ERM is sub process of overarching MS.

Yes, but depends on maturity of existing MS in terms of when to integrate

- need to filter to enable delving as deep into a specific MS as required by the standard

Part B) No, ERM is broader than EH&S eg. includes finance security, etc.

5. Are the individual approaches or systems to manage a range of corporate risks consistent and should, or can, they be unified?

- Yes, should be consistent, in terms of principles across the organizations - should be aligned with ERM

  - system & process need enough flexibility to effectively manage different issues

  - need to hit right level prescription

Unified risk matrix is a good approach

- how is risk ranking / weighting between different subjects eg. environment vs. Health and safety resolved

- *need to evolve to the aforementioned ^^

Yes, should be consistent in terms of development and implementation

- can evolve to be user friendlier

- fosters buy in 1 process -> ease of understanding -> more effective use

- common message and language needed - keep it in term so readily understood

6. How would an internal audit program established for an EMS/EH& SMS have to be modified to address and ERM? The internal audit program including scheduling, locations, auditor qualifications/knowledge, workload, etc., etc., etc.

Need to broaden scope.

- all issued need to be revisited in terms of resourcing, competency, consideration of audit fatigue
- Assess risk & priority areas from a more holistic standpoint
- Provides opportunity to assess the overall corporate risk assessment process
- Audit process, tools, plans may need to be revisited
    - need to consider objectives from ERM standpoint
    - how does audit program need to be modified?
    - appropriate emphasis on ERM eg. risk based audits.
    - need to develop protocols to manage ERM
    - change scope of existing audit program
    - possible changes to audit eg. action planning to handle

Non-conformities:

- risk management - considers full suitability of control tools, to ensure risk is controlled / mitigated to within tolerance.

- controls need to be in place + need to identify risk and assess risk

- process of aligning controls related to specific MS to ERM

- linkage of MS controls -> ERM

Should audits address one or all types of risk?

a) inherent risk

b) residual

c) or magnitude of risk reduction achieved by controls

- Start with inherent - rest falls out.
- High level of inherent may have good controls therefore if only consider residual may drop off list & shift audit focus to residual which may not be appropriate. Need to consider the degree of risk.
- Also need to assess effectiveness of controls applied to inherent to ensure continuing effectiveness
- Audit detection risk - ie. risk that audit program won't identify risk
- Business process should not rely on audit as only line of defence - No management by audit!
- A robust risk based audit program is critical to overall management of risk
- Need to accommodate expectations of Board of Audit Risk Committee.
- Should also engage client & auditees in providing input.