SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Risk Assessment Workshop

1. IIA Standards
2. IIA Practice Advisories
3. PEM-PAL Manual Template
4. Example

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

2010 Planning

The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

Interpretation:

The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consultation with senior management and the board.

OECD

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Practice Advisory 2010-1: Linking the Audit Plan to Risk and Exposures

1. Develop or update the audit universe: a list of all the possible audits that could be performed. The CAE may obtain input on the audit universe from senior management and the board.

2. The audit universe can include components from the organization's strategic plan. It will consider and reflect the overall business' objectives. The audit universe will normally be influenced by the results of the risk management process.

3. The CAE prepares the internal audit activity's audit plan based on the audit universe, input from senior management and the board, and an assessment of risk and exposures affecting the organization.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Practice Advisory 2010-1: Linking the Audit Plan to Risk and Exposures

4. It is advisable to assess the audit universe on at least an annual basis to reflect the most current strategies and direction of the organization. In some situations, audit plans may need to be updated more frequently (e.g., quarterly) in response to changes in the organization's business, operations, programs, systems, and controls.

5. A variety of risk models exist. Most risk models use risk factors such as impact, likelihood, materiality, asset liquidity, management competence, quality of and adherence to internal controls, degree of change or stability, timing and results of last audit engagement, complexity, and employee and government relations.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning

1. Risk management is a critical part of providing sound governance that touches all the organization's activities. Management typically uses a risk management framework to conduct the assessment and document the assessment results.

2. Implementation of controls is one common method management can use to manage risk within its risk appetite. Internal auditors audit the key controls and provide assurance on the management of significant risks.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning

3. Two fundamental risk concepts are inherent risk and residual risk.

4. Key controls can be defined as controls or groups of controls that help to reduce an otherwise unacceptable risk to a tolerable level:

   - a significant reduction from inherent to residual risk
   - controls that serve to mitigate a large number of risks.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning

5. Internal audit planning needs to make use of the organizational risk management process, where one has been developed.

6. Specialized expertise may be needed.

7. Internal auditors make an assessment of the organization's risk management process and determine what parts can be used in developing the internal audit activity's plan.

8. In addition, the internal auditor coordinates with other assurance providers and considers planned reliance on their work.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning

9. The internal audit charter normally requires the internal audit activity to focus on areas of high risk, including both inherent and residual risk. The internal audit activity needs to identify areas of high inherent risk, high residual risks, and the key control systems upon which the organization is most reliant. If the internal audit activity identifies areas of unacceptable residual risk, management needs to be notified so that the risk can be addressed.

10. Internal auditors also try to identify unnecessary, redundant, excessive, or complex controls that inefficiently reduce risk. In these cases, the cost of the control may be greater than the benefit realized and therefore there is an opportunity for efficiency gains in the design of the control.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning

11. To ensure relevant risks are identified, the approach to risk identification is systematic and clearly documented.

12. Many organizations have developed risk registers that document risks.

13. Some organizations may identify several high (or higher) inherent risk areas. While these risks may warrant the internal audit activity's attention, it is not always possible to review them.

14. A selection of lower risk level business unit or branch type audits need to periodically be included in the internal audit activity's plan to give them coverage and confirm that their risks have not changed.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning

15. An internal audit activity's plan will normally focus on:
    - Unacceptable current risks where management action is required. These would be areas with minimal key controls or mitigating factors that senior management wants audited immediately.
    - Control systems on which the organization is most reliant.
    - Areas where the differential is great between inherent risk and residual risk.
    - Areas where the inherent risk is very high.

16. When planning individual internal audits, the internal auditor identifies and assesses risks relevant to the area under review.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

2010 Planning

2010.A1 The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

2010.A2 The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

2010.C1 The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Proposed Change to Standard 2010

The chief audit executive must establish ***a risk-based plan~~s~~ to determine the priorities of the internal audit activity, consistent with the organization's goals.***

Interpretation:

The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after ~~consultation with senior management and the board~~ consideration of input from senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

PEM-PAL Manual on Audit Universe

- Totality of auditable processes, functions and locations
- Horizontal or vertical approach
- Key processes
- Critical control areas
- Manageable components
- Dynamic universe

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

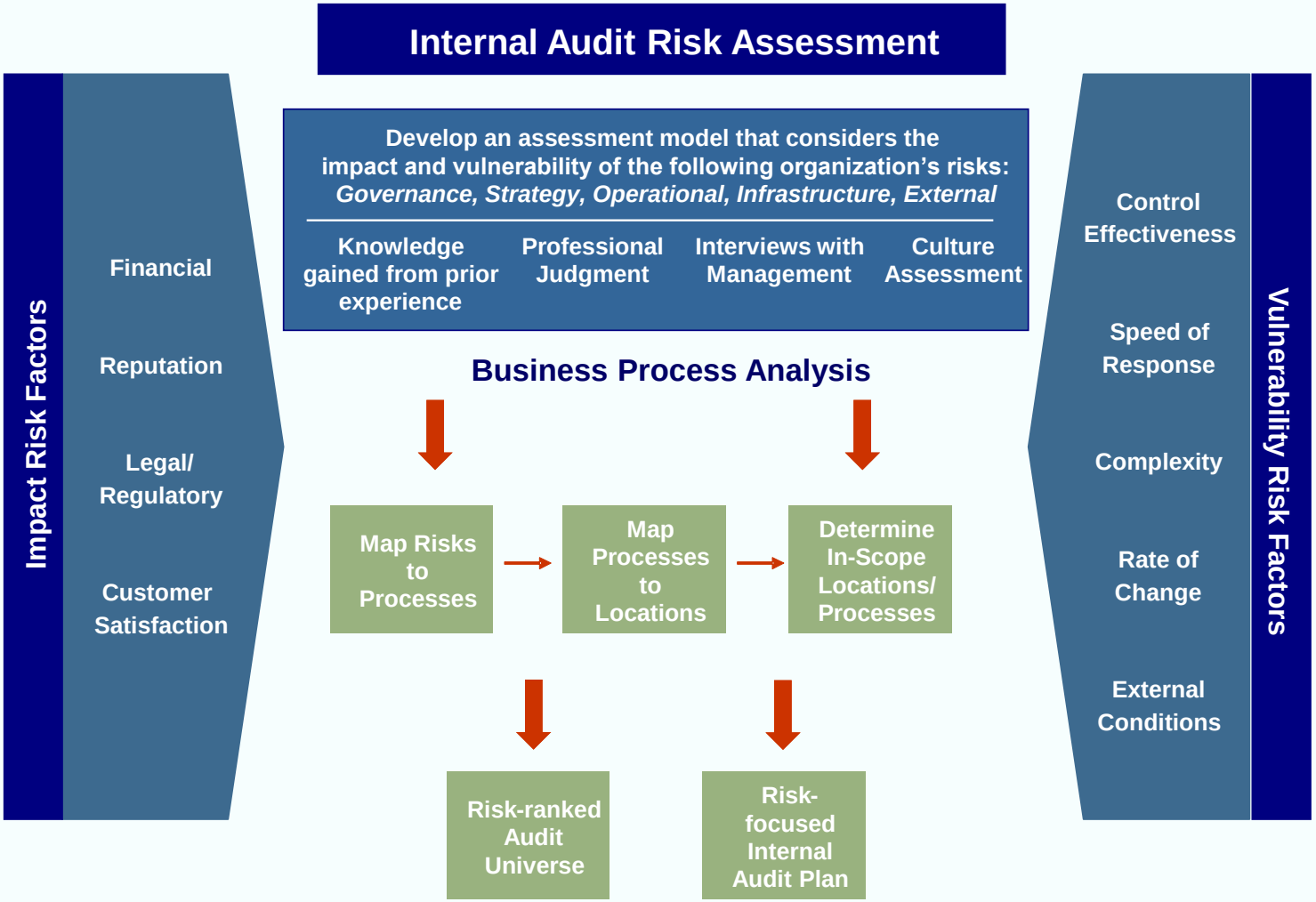
PEM-PAL Manual on Risk Assessment Methodology

- Definition of risk categories: define which risks are going to be assessed.
- Definition of risk criteria for impact and probability (vulnerability?).
- Definition of risk scoring content: in which situation is a risk going to be scored high, medium or low? (middle scores!)

Risk Assessment Methodology and Approach

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU



SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Risk Framework

A risk framework is used to map the identified key risks into the major risk categories, to ensure that all categories of risks have been covered

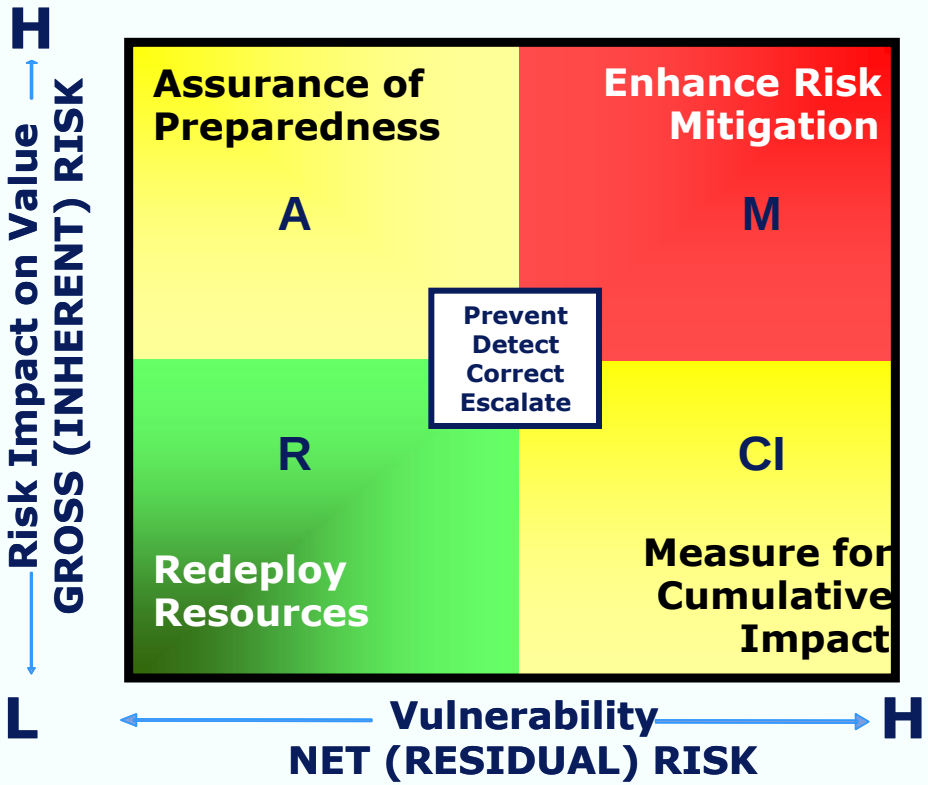
Risk Prioritization – Impact criteria (examples)

IMPACT	FINANCIAL	REPUTATION	LEGAL / REGULATORY	CUSTOMER SATISFACTION	CAPACITY
High	Risks that can create losses > approx. 3% of the operating revenue.	National and international press coverage.	Significant actions (e.g. fines, penalties) imposed by the European Commission, local government etc.	Significant impact on the achievement of customer (internal or external) satisfaction goals / metrics	Significant impact on the capacity of the organization to change (processes, organization, systems, products etc.)
Medium	Risks that can create losses between 0,5% and 3% of the operating revenue.	Escalating community or customer group activism, regional press coverage.	Any governmental and/or regulatory authorities' scrutiny and/or customer action.	Moderate impact on the achievement of customer (internal or external) satisfaction goals / metrics	Moderate impact on the capacity of the organization to change (processes, organization, systems, products etc.)
Low	Risks that can create losses < approx. 0,5% of the operating revenue.	Local press coverage.	Any customer scrutiny.	Very low impact on the achievement of customer (internal or external) satisfaction goals / metrics	Very low impact on the capacity of the organization to change (processes, organization, systems, products etc.)

Risk Prioritization – Exposure / Vulnerability criteria (examples)

VULNERA-BILITY	PREVIOUS RISK EXPERIENCE	PERVASIVENESS	CAPABILITY (PEOPLE)	CAPABILITY (PROCESSES)	CAPABILITY (SYSTEMS)
High	High previous adverse risk experience.	Risk affects a high number of transactions and/or processes.	A limited number of key staff or staff with limited competency to manage the risk.	Process controls do not exist or do not operate as designed.	System controls do not exist or do not operate as designed.
Medium	Moderate previous adverse risk experience.	Risk affects a moderate number of transactions and/or processes.	A limited number of key staff or staff with moderate competency to manage the risk.	Process controls are operating effectively as designed, but design can be improved.	System controls are operating effectively as designed, but design can be improved.
Low	Low previous adverse risk experience.	Risk affects a low number of transactions and/or processes.	Most staff has high competency to manage the risk.	Process controls are designed, implemented and operate effectively.	System controls are designed, implemented and operate effectively.

Prioritize Risk – Risk Map



- **Mitigate** – Management strategies to reduce or minimize the impact of or the vulnerability to a risk
- **Assure** – Increased level of confidence that risk exposures are within the organization's Risk Appetite
- **Redeploy Resources** – Determine if risk management resources are better deployed elsewhere
- **Cumulative Impact** – Investigate further to determine the aggregate impact of a number of small impacting risks

	B	C	D	E	F
1	**Auditable Segment**	**Risk Category**	**Risk Score**	**Budget Hours**	**Recommended for Internal Audit Plan**
2	Information Systems Integration/Consolidation	High	520	300	✓
3	Business Continuity/Disaster Recovery Plan	High	520	300	
4	Claims Processing	High	500	300	✓
5	Regulatory Investigations	High	500	200	
6	HIPAA	High	480	150	✓
7	New Systems Development	High	480	200	✓
8	Information Systems Control & Security	High	460	250	
9	Pharmacy Claims Processing	Medium	440	300	✓
10	Treasury	Medium	440	250	✓
11	Reserving	Medium	400	150	
12	General Computer Controls	Medium	400	100	✓
13	Litigation	Medium	380	150	
14	Risk Relationships - Contract Compliance	Medium	380	200	
15	Billings and Collections	Medium	380	250	
16	Application Level Controls	Medium	380	100	✓
17	Broker Commissions	Medium	360	200	✓
18	General Accounting	Medium	360	150	
19	Accounts Payable (Trade)	Medium	360	250	
20	Finanical Accounting Controls	Medium	360	200	
21	Human Resources Regulatory Compliance	Low	340	200	
22	Budgeting	Low	340	150	
23	Compensation & Benefits	Low	320	200	
24	Procurement	Low	320	250	
25	Administrative Services	Low	300	150	
26	Corporate Communication	Low	300	150	
27	Special Projects	Not Rated	0	150	✓
28	Administrative (Audit Comm./Meetings)	Not Rated	0	100	✓
29	Audit Universe & Risk Assessment	Not Rated	0	150	✓
30	Management and Supervision	Not Rated	0	100	✓

SIGMA

A joint initiative of the OECD and the European Union, principally financed by the EU

Conclusion

- We first need to develop a proper audit universe.
- Secondly, proper risk criteria shall be used. No complex mathematical model needed.
- Finally, the results of our risk assessment shall make sense to the auditors and to management.