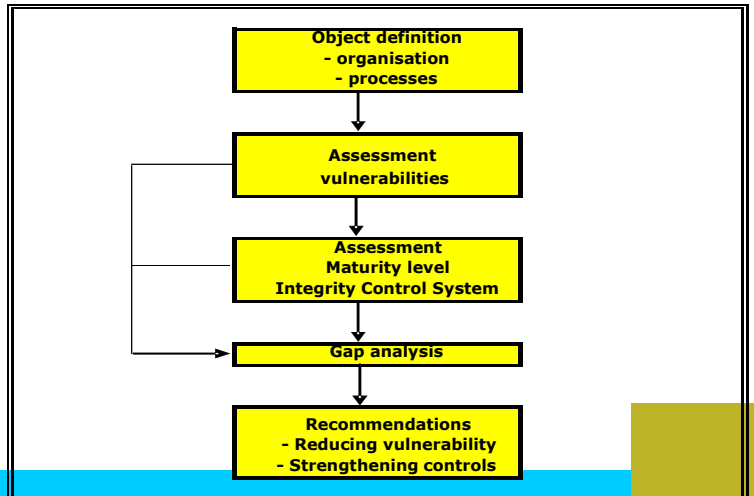
Algemene Rekenkamer

Assessing INTegrity
Workshop

Algemene Rekenkamer | Postbus 20015 | 2500 EA Den Haag

Algemene Rekenkamer

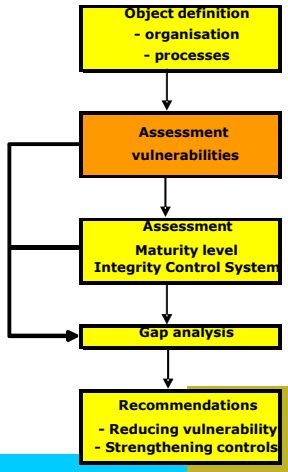
AINT methodology



Algemene Rekenkamer

Assessment of vulnerabilities

- What are the inherent vulnerabilities?
- What are vulnerability enhancing factors?
- What is the vulnerability profile?



3

2

Algemene Rekenkamer

Inherent vulnerabilities

Elements	Vulnerable areas /activities /actions	
Relationship of the entity with its environment	Contracting	procurement, tenders, orders, assignments, awards
	Payment	subsidies, benefits, allowances, grants, sponsoring
	Granting / Issuance	permits, licenses, identity cards, authorizations, certificates
	Regulating	conditions of permits, setting standards / criteria
	Inspection / audit	supervision, oversight, control, inspection, audit
	Enforcement	prosecution, justice, sanctioning, punishment
Managing public property	Information	national security, confidential information, documents, dossiers, copyright
	Money	treasury, financial instruments, portfolio management, cash/bank, premiums, expenses, bonuses, allowances, etc.
	Goods	purchasing / selling, management and consumption (stocks, computers)
	Real estate	buying / selling

4

4

Algemene Rekenkamer

Vulnerability enhancing factors

Complexity

Change / dynamics

Management

Personnel

Problem history

5

5

Algemene Rekenkamer

1. Complexity

Innovation / advanced computer systems
Complex legislation
Special constructions (legal / fiscal)
Bureaucracy
Lobbying
Networks of relations
Mix of public-private interests (commerce / competition)
Need for external expertise
Political influence/ intervention

6

6

Algemene Rekenkamer

2. Change / dynamics

Young organisation
Frequently changing legislation
Strong growth or downsizing
Privatisation, management buy-out
Outsourcing
Crisis (reorganisation, threats with huge impact, survival of the organisation or job at stake)
External pressure (pressure on performance, expenditure, time, political pressure, shortages / scarce resources in comparison with duties)

7

7

Algemene Rekenkamer

3. Management

Dominant
Manipulative
Formal / bureaucratic
Solistic operation
Remuneration strongly dependent on performance
Lack of accountability
Ignoring advice / signals
Defensive response to criticism or complaints

8

8

Algemene Rekenkamer

4. Personnel

Work environment/ loyalty	Pressure on performance / income dependent on performance
	Low status / lack of esteem/ low rewards / low career prospects
	Poor working conditions/ high workload
	Group loyalty
	Power to obstruct
Individual	Having other interests (side jobs, etc.)
	Personal debts
	Lifestyle (overspending)
	Personal secrets (vulnerable for blackmail)
	Personal threats
	Addictions (alcohol, drugs)

9

9

Algemene Rekenkamer

5. Problem history

Complaints
Gossip and rumors
Signals / whistle blowers
Earlier incidents (recidivism)
Administrative problems (backlogs, inconsistencies, extraordinary trends)

10

10

Algemene Rekenkamer

Vulnerability profile

Vulnerability Enhancing factors / Inherent vulnerability	Low	Medium	High
Low	low	low	**Medium**
Medium	**Medium**	**Medium**	HIGH
High	HIGH	HIGH	HIGH

11

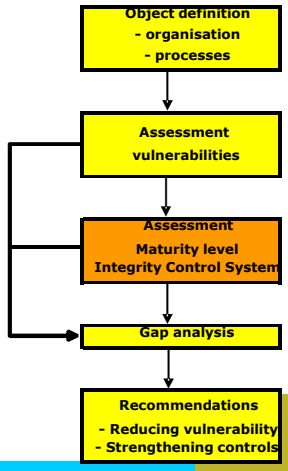
11

Algemene Rekenkamer

Assessment maturity level Integrity Control System

What is the maturity level of the integrity control system?

- Existence of controls
- Operation of controls
- Effectiveness of controls



12

12

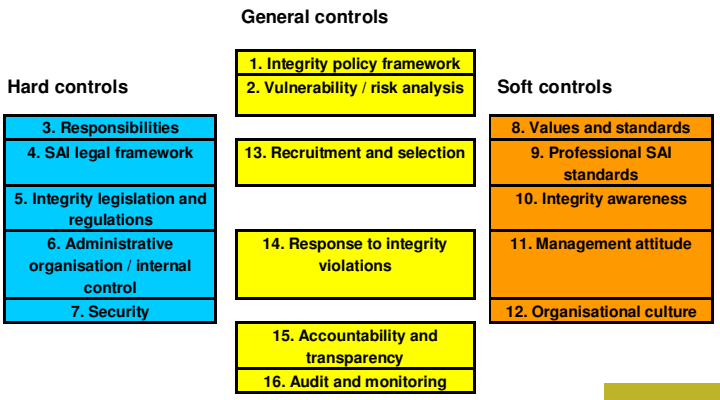
Algemene Rekenkamer

Preventive measures

- What could have been done to prevent this incident?
- What measures did the organisation take?
- What else could they do?
- What could others do?

Algemene Rekenkamer

Integrity Control System



Algemene Rekenkamer

Maturity levels

Level	Criteria
0	- The measure does not exist
1	- The measure exists - The measure is not implemented / observed
2	- The measure exists - The measure is implemented / observed - The measure is not effective
3	- The measure exists - The measure is implemented / observed - The measure is effective

15

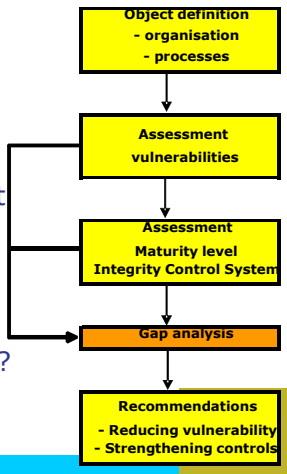
15

Algemene Rekenkamer

Gap analysis

Match integrity control system with established vulnerabilities

- What is the vulnerability profile?
- What are the most important vulnerable processes?
- Does the integrity control system protect the organisation against these integrity vulnerabilities/risks?
- What are the remaining vulnerabilities?



16

16

Algemene Rekenkamer

Recommendations

Reducing vulnerability

1. …
2. …
3. …

Improving Integrity control system

1. …
2. …
3. …

17

Algemene Rekenkamer

Group work

- Describe an example of a case where an organization was confronted with (an) integrity incident(s)
  - What organization?
  - What happened?
  - How was it discovered/disclosed?
  - Who were involved?
  - What impact did it have?
  - How did the responsible management react?
  - Was there any follow-up?

Algemene Rekenkamer

What inherent vulnerabilities can you recognize in the case under discussion?

Algemene Rekenkamer

What enhancing factors can you recognize in the case under discussion?

Algemene Rekenkamer

What could have helped to prevent the incident or mitigate the impact in the case under discussion?

Algemene Rekenkamer | Postbus 20015 | 2500 EA Den Haag

21

Algemene Rekenkamer

Recommendations

Reducing vulnerability

1. …
2. …
3. …

Improving Integrity control system

1. …
2. …
3. …

22