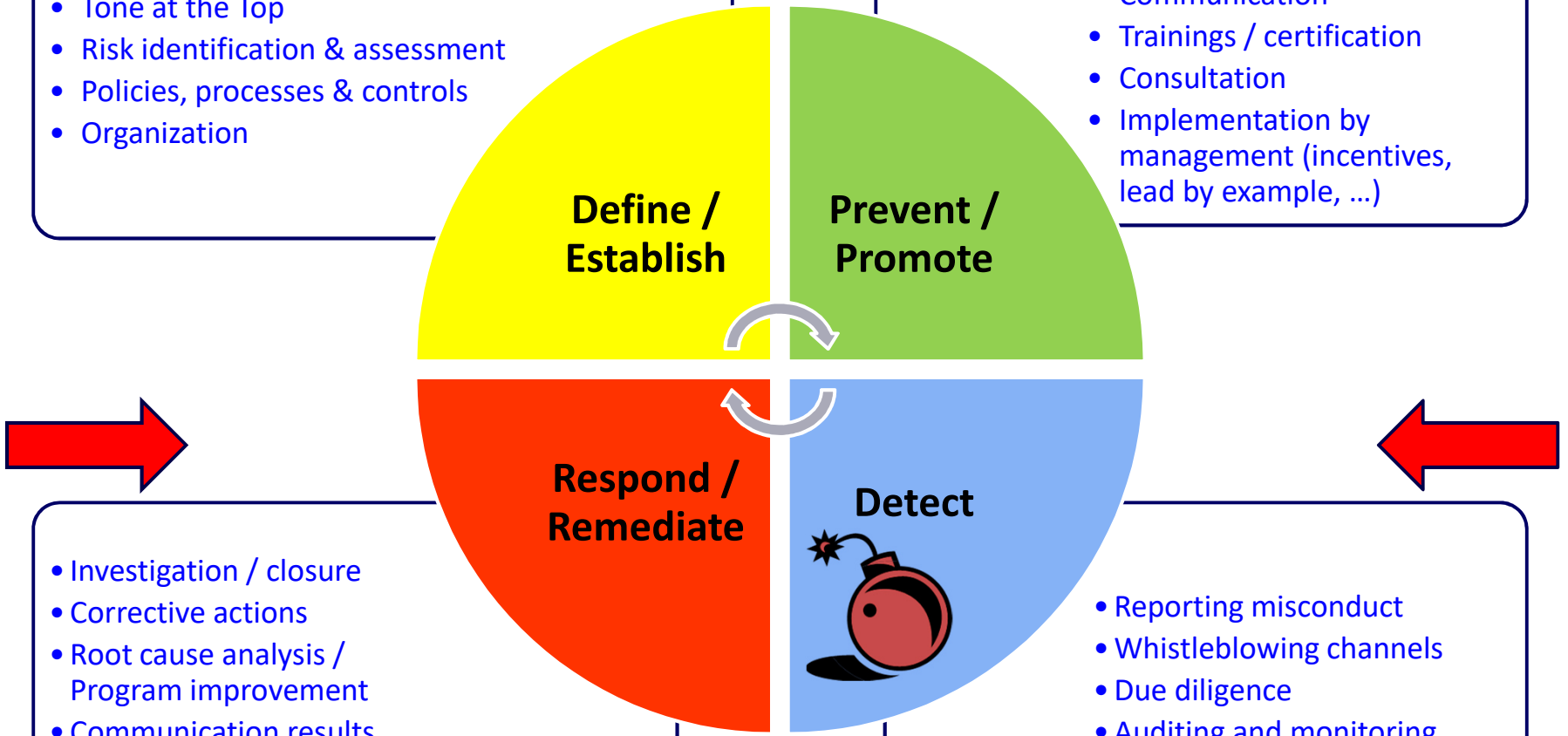
Learning from a Compliance Lapse

CAS Compliance Management – April 14, 2016

Stefano Caldoro

Compliance program

- Tone at the Top
- Risk identification & assessment
- Policies, processes & controls
- Organization



- Communication
- Trainings / certification
- Consultation
- Implementation by management (incentives, lead by example, …)

- Investigation / closure
- Corrective actions
- Root cause analysis / Program improvement
- Communication results

- Reporting misconduct
- Whistleblowing channels
- Due diligence
- Auditing and monitoring

A maxim for the learning process

γνῶθι σεαυτόν

Know yourself

Take insight into your development opportunities
and then improve yourself

like the personal development maturity process or the immune system

Siemens lessons learned

Beginning in the mid-1990s until 2007, Siemens engaged in broad and systematic practices of making payments to customers for the purpose of obtaining business. The overall involved amount was approx. EUR 1.3 billion. Siemens paid USD 1.6 billion fines and USD 900 million external advisors' fees and expenses (additionally, there were separate judgments against individuals).

- *Management*: replaced 80% of the top level executives, 70% of the next level down and 40% of the middle management with outsiders
- *Governance*: Change of the way to take decisions at the managing board (more operations knowledge and governance control)
- *Operations*: Simplified global operating units (closer and easier control from HW)
- *Compliance*: Strengthening of legal and compliance (Organization: 600 employees in compliance dpt.; Culture: full integration of compliance program in all business; Policies, processes and controls: tailored and risk-based)
- *Competitive business*: Focus on new competitive business (e.g. green portfolio)

ThyssenKrupp lessons learned

In the last years ThyssenKrupp has been involved in a long series of scandals about price fixing of railway track (2011/12) as well in the in the auto industry (2013), mismanagement and embezzlement, misappropriation of company funds for luxury joyrides for journalists and workers' representatives (2011/12), , corruption in particular in the eastern European area, at the former marine venture, etc.

ThyssenKrupp had to pay multimillions penalties as well as damages third parties.

Also ThyssenKrupp learned:

- *Change of management*
- Systematical *increasing of legal and compliance organization* since 2011 (over 50 employees at the headquarters and 15 local compliance officers)
- *Operational integration* of the compliance organization
- Offering of *immunity* to its employees to resolving compliance failures

Incident response and damage control

When a lapse is detected, answer four questions before getting back to a stable state:

1. What and how happened? → Detailed impartial analysis

2. What are the effects? → Analysis of the potential effect to the financial, operational, reputation and regulatory exposure of the organization (early estimation to be fine-tuned during the investigation process, if this is needed)

3. Is it still happening? → What are the immediate measures for terminating the issue and limit damages?

4. What are the necessary corrective measures? → Analysis of the recovery steps; these shall be adequate to the individual case and focused on the core elements of the compliance laps

Case investigation

Types: (a) Legal due diligence; (b) Internal process /controls audit

Principles: Confidentiality, anonymity, protection from retaliation (full and fair process for everyone involved), timeliness, investigators' integrity and competence.

Case based considerations / decisions:

- Roles (CCO, Legal, Int. Audit, IT, HR, local management, external advisors …)
- Timelines
- Local laws on employment, data protection, criminal procedure etc.
- Secrecy (controlling rumors)
- Ensuring evidence and documentation / Formulating the best possible defense against accusations
- Disclosure illegal activities to authorities (in case, applying for immunity, leniency)
- Corrective and disciplinary actions

Case related corrective actions / 1

Employee

- Disciplinary actions (from warning, required compliance course and counseling, forfeiture of compensation elements, up to suspension, demotion, dismissal)?
  - According to disciplinary policy (panel takes measure, in general HR and senior management supervisors; notice of concern and rights of defense)
  - Aggravating factors (repeat offender, fails to cooperate, manager position, involved others, was trained, refused to train or ignored legal advice)
- Legal action?

Supervisors

- Measures against supervisors who failed to apply controls / prevent misconduct

Case related corrective actions / 2

Involved business partners

- Open discussion and cooperative correction of business structure?
- Termination?
- Legal action against business partner and/or its employees?

Authorities

- Information / Voluntary disclosure?
- Legal actions? Criminal complaints?

Communication

- Managing communication with other business partners
- Managing media inquires

Case closure

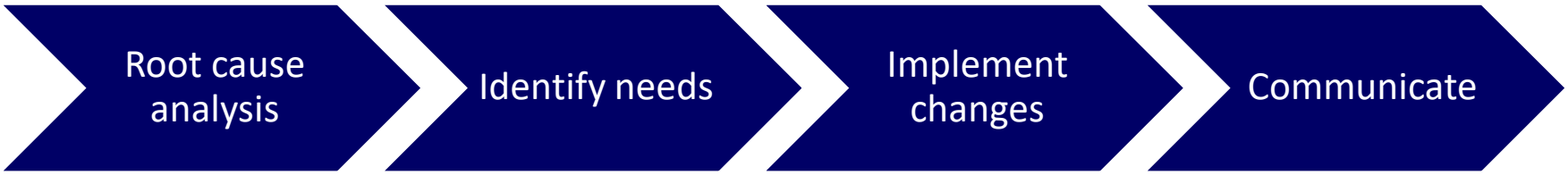
- Document all steps from detection to corrective / disciplinary measures.
- Report compliance breaches to the senior management / include them in the compliance report.
- Use any lapse as a lessons learned for uncovering gaps and deficiencies in the program and eliminating them.

Program improvement

Manage risks, not only events

Once the problem is resolved, you are only halfway as you have only managed the specific event, not the related risk that such event can happen again.

- Ongoing improvement of a compliance program: A mature organization shall not quiet lapses to avoid embarrassment or responsibility; it must learn as much as possible from mistakes for improving the program and the whole organization.
- Purpose: Prevent lapse repetition (regulators expect prevention by a compliance program modification; if failures continue they assume the program is ineffective)
- Process:



Root cause analysis / 1

Effective safeguards for prevention of reoccurrence can be found only through the understanding of the underlying reasons of a failure (Root cause analysis).

1. Is the failure related to missing processes and controls (design deficiency)?

2. Is the failure related to insufficient processes and controls (design deficiency)?
   - The risk or its effect were underestimated or misunderstood (incorrect, incomplete, unclear, obsolete risk identification, risk assessment and/or instructions);
   - monitoring, reporting and sanctions are not sufficiently included in the controls design;
   - there is no effective discipline for violations.

3. Did the processes and controls fail (operational deficiency)?
   - The processes and controls were designed correctly, but were not implemented;
   - They do not function correctly or the way they were designed;
   - They were not (correctly) communicated.

Root cause analysis / 2

4. Are the detection and responding mechanisms in place sufficient and effective? Was the lapse detected by chance? Could it have been detected earlier?

5. Irrespective of a formal gap in the processes and controls, is the failure related to ignorant unintentional behavior, negligence or (individual or systematic) willful intent (substantial failure)?

Responsibility: *Panel of experts* (e.g. internal audit, compliance, legal) with the support of *management and concerned key operations representatives* as well as *external advisors* (e.g. forensics for corruption, data analytics providers for insider trading, privacy experts for data breach, …)

Needs identification / 1

Based on the root cause analysis information, the effect of the specific event and the recovery effort required,

(a) identify the changes needed in the compliance program, in particular regarding

- the organization's risk profile (problematic locations and geographical areas; job functions, business units and industries, etc.)
- the processes and controls (design / operational improvements) and
- other specific instruments for prevention, information, detection and response;

(b) generate recommendations on specific new compliance requirements and improvements focused on core elements of the compliance failure, e.g. regarding *[… (i) to (v)]*

Needs identification / 2

(i) risk map: updating risk identification and assessment, planning consistent evaluation of their effectiveness;

(ii) rules: improving or introducing new policies & guidance materials, processes and controls;

(iii) IT technology: introduction of controls tools, e.g. for (aa) testing, reviewing and monitoring the controls; (bb) performing, consolidating, monitoring assessments, surveys or questionnaires; (cc) providing information on legal, regulatory updates or compliance situations;

(iv) influencing behavior/understanding:

- culture and knowledge improvement → more tone at the top, break the "permafrost" in the middle management
- more/better trainings and communication (face-to-face for high risk),
- incentive systems / efficiency improvement of sanctions systems;

Needs identification / 3

(v) organization change:

- operative organization
  - management, operative business (termination / rotation / reassignment …)
  - third parties (other / insourcing)
- compliance organization
  - change and/or new expert resources (internal / external)
  - Improvement of the reporting lines / access to top management
  - governance on the organization of compliance activities: map deliverables, ways of interaction with operations and other support functions

Changes implementation

Define / Establish

After having identified what needs to be changed,

- the panel reports the documented results and recommendations to senior management / decision makers for implementation;
- the senior management / decision makers implement the changes needed (otherwise, not acting on recognized gaps can be a liability and the risk of repeating the lapse will remain unchanged leading to further liability; not acting on recommended changes is a waste and the people's respect for the analytic process will be killed after going through all of that work):
  1. Remedial measures in work plans (responsibilities, roles, timing, expected results, measurement process)
  2. Execution by accountable personnel appointed for this purpose
  3. Effectiveness measurement by internal audit

Documentation

All steps from analysis to the implementation of the corrective actions and changes shall be documented in order to fully capture the institutional learning that comes from these analyses and provide tangible evidence.

Communication of lapses

Prevent / Promote

1. Organizations have to communicate and discuss openly (at meetings, with presentations, internal communications, …)
   - the circumstances of compliance failures involved (what and how)
   - why the failures happened
   - the disciplinary actions taken (e.g. employee terminations, but not the information about the employees and others who were disciplined)
   - what to do to ensure and what has been implemented that it does not happen again (results of the root cause analysis and needs identification)

2. Use the lapse and the analysis results as lessons learned in trainings and during specific consultation.

Mock case A

A supplier has invited the sales responsible Tim to its annual customers' event including dinner, overnight stay and a ticket to a sport event for the same night (not adequate acc. to company policy). His predecessor participated regularly.

Tim is not sure and asks the local managing director who confirms this is not be a problem. Tim looks at the company policy and asks the CCO.

Detection:
- Prior approval
- Compliance advice

- Prohibition to participate / Communication to supplier
- Analysis previous cases
- Information to supervisor of local MD on facts

Remedial measures:
- Adequate response
- Case-based corr. action

- Root cause analysis → operational deficiency

- Identification needs

- Local trainings / Improved monitoring

- Change implementation

Mock case B / 1

Martin, the head of sales in Russia, has participated to an event at a trade association where information on members' prices and future market behaviour was shared. He informs his team on the topics discussed at the event at the team meeting and writes the minutes. Although the company has published a due diligence process for participation to trade associations' events, the legal dpt. / CCO were not informed.

In the course of a regular internal audit the auditor sees the invitation to the events and the minutes. He asks whether the legal dpt. was involved for mandatory consultation acc. to policy and informs CCO.

Detection:
- Audit

Mock case B / 2

- Interviews of team members (confirm intentional behavior)
- Legal due diligence assessment (with local external lawyer) with the documents collected by internal audit
- Decision on voluntary disclosure to authorities
- Management of communications with association members (prevent others' immunity application before end investigation)
- Change of market behavior
- Disciplinary measures with employees (in particular Martin)
- Report

Remedial measures:
- Adequate response
- Case-based corr. action

Mock case B / 3

- Root cause analysis →
  - substantial failure: intentional failure to follow prohibition
  - operational deficiency: failure to involve legal dpt.;
  - design deficiency: missing explicit process and controls

- Identification risk profile of business unit in Russia; specific processes and controls shall be implemented

- New risk assessment
- Additional guidance materials for local team (dd process for participation to events in Russian and more detailed)
- Warning message by top management
- Local face-to-face trainings
- Job rotation
- Improved monitoring
- Work plan / execution / documentation / publication

- Identification needs

- Change implementation

Mock case C / 1

A sales company has been selling for years dual use machines to various customers in Turkey and Pakistan with the respective Swiss export licenses. The customers resell the machines to an end customer in Iran. The managing director and his sales team are aware that the machines do not remain in Turkey and Pakistan, but they close an eye. Maintenance services are provided to the end customers through a third party in UEA. The true deal structure does not appear in the business and financial documentation.

Neither the sales company nor the procurement/logistics team at the manufacturing/ assembling plant are aware that the machines include US origin components subject to export limitation to Iran.

Bruno, a team member, is concerned and uses the whistleblowing channel.

Detection:
- Whilstleblowing

Mock case C / 2

What to do?

-
-
-
-
-
-
-
-
-
-
-

Remedial measures:
- Adequate response
- Case-based corr. action

Remedial measures:
- Identification needs
- Change implementation

Thanks for your attention!

Dr. Stefano Caldoro LL.M.
Corporate Compliance Officer

stefano.caldoro@georgfischer.com
+41 52 631 24 47

Georg Fischer AG
Amsler-Laffonstrasse 9
CH-8200 Schaffhausen

As of October 1, 2016

Dr. Stefano Caldoro LL.M.
Rechtsanwalt / Partner

caldoro@lanter.biz
+41 44 250 20229

LANTER
Seefeldstrasse 19
CH-8032 Zurich