Auditing Risk Culture

Zuzana Kitto
UniCredit Bank
IIA Czech Republic

Welcome to
UniCredit

Obsah

- What is risk culture?

- How should Internal Audit assess risk culture?

What is Risk Culture? There are many definitions...

Project Management Institute:

Culture arises from **repeated Behaviour** – if we do the same things repeatedly we will develop a shared approach to "how we do things around here." But Behaviour is based on our underlying Attitudes – how we think shapes our actions

Institute of Risk Management:

"An effective risk culture is one that enables and regards individuals and groups for taking the right risks in an informed manner. "

European Banking Authority:

"Institution's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management and the controls that shape decisions on risks. "
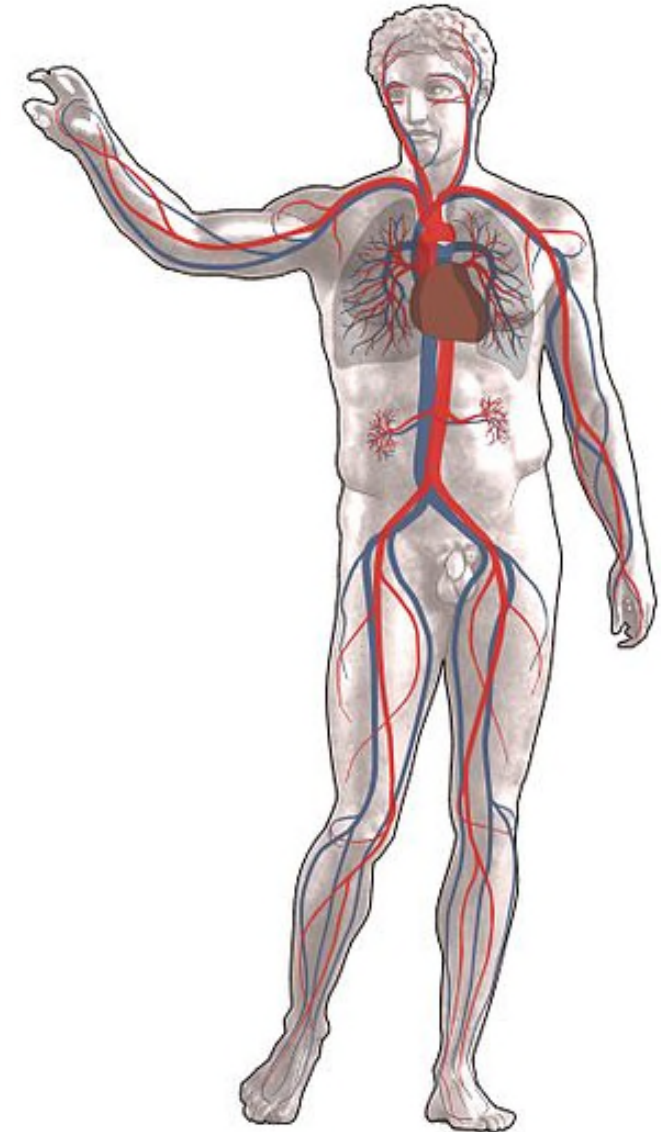
Why Risk Culture matters? Well Fargo case (Sept 2016)

Wells Fargo Fined $185 Million for Fraudulently Opening Accounts

An analysis conducted by a consulting firm hired by Wells Fargo concluded that bank employees opened up over 1.5 million deposit accounts that may not have been authorized, according to the CFPB.

The way it worked was that employees moved funds from customers' existing accounts into newly-created accounts without their knowledge or consent, regulators say.

Additionally, Wells Fargo employees also submitted applications for 565,443 credit-card accounts without their knowledge or consent, the CFPB said the analysis found.

The CFPB said Wells Fargo had "terminated roughly 5,300 employees for engaging in improper sales practices." The bank said in a press release that after a third-party review dating to 2011, $2.6 million had been refunded to customers, who received an average of $25.

The bank said firings included managers, and that it was making investments "in enhanced team-member training and monitoring and controls."

A 2013 **LA Times** investigation found a culture that left some employees desperate to reach quotas, whether it was forging signatures or begging family members to open additional accounts.

Wells Fargo branch manager Rita Murillo came to dread the phone calls.

Regional bosses required hourly conferences on her Florida branch's progress toward daily quotas for opening accounts and selling customers extras such as overdraft protection. Employees who lagged behind had to stay late and work weekends to meet goals, Murillo said.

4 elements of risk culture

Tone from the Top

■**Top at the top**: the board and senior management are the starting point for setting the core values and expectations for the risk culture of the company, and their behaviour must reflect the values being espoused.

Accountability

■**Clear accountability**: relevant employees at all levels understand the core values of the company and its approach to risk, are capable of performing their prescribed roles, and are aware that they are held accountable for their actions in relation to the company's risk-taking behaviour.

Effective Communication

■**Effective communication and challenge**: decision-making processes encourage a range of views; allow for testing of current practices; stimulate a positive, critical attitude among employees; and promote an environment of open and constructive engagement.

Incentives

■**Incentives framework**: performance and talent management encourage and reinforce maintenance of the company's desired risk management behaviour. Financial and non-financial incentives support the core values and risk culture at all levels of the company.
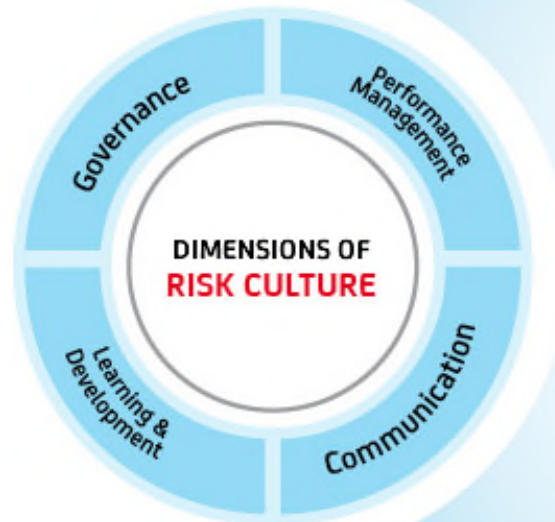
European Banking Authority - New Guidelines on Internal Governance

- new Guidelines published in September 2017, effective from 30 June 2018

- additional requirements of risk culture as one of the main drivers of the new edition

- appropriate risk culture should encompass:

  - Tone from the top

  - Accountability

  - Effective communication and challenge

- other regulators of financial institutions around the world:

  - Financial Stability Board

  - Basel Committee on Banking Supervision

  - UK, US, Holland, Australia

UniCredit Risk Culture

DIMENSIONS OF RISK CULTURE

- Governance
- Performance Management
- Learning & Development
- Communication

GOVERNANCE

Setting the UniCredit risk appetite, thus ensuring that our Group strategy is driven by the level of risk we want to take Creating a link between compensation mechanisms and our risk appetite

Strengthening risk policies and processes

PERFORMANCE MANAGEMENT

Enhancing guidelines for risk-based incentive systems

Rewarding servicing the greater, long term interests of our Group and our clients through financial and non financial incentives

LEARNING & DEVELOPMENT

Linking progressive level of competence in risk management to professional development

Offering risk learning programs, both on-line and in classroom

Ensuring and increasing job rotation between control functions and business lines

Assessing credit and risk management skills in appointment processes for key positions

COMMUNICATION

Reiterating the importance of risk culture starting from top management endorsement and cascading down in the organization

RISK ACADEMY: MIND THE RISK, LEAR[N]

The training and learning offer is wide and it has been shaped t[...]

RISK DIPLOMA PATH
For all the professionals who wish to have a comprehensive view on risk

RISK MANAGEMENT LEARNING LAB
For managers who wish to further strengthen their knowledge on risk management

And What About Internal Audit?

Interviews with Internal Audit Directors

- the most important is "**Tone at the Top**" of the Board and Group / owners

- each IA function performs assessment of risk culture, directly or indirectly:

1. **As part of each audit** - included typically in control environment assessment

2. As part of **annual assessment** of the internal control system; however, often only implicitly rather than explicit statement. Internal Audit is not able to get underlying information from audits/elsewhere to provide a structured assessment

3. In **specific audits** dedicated to risk culture elements

   ➢ fraud investigations / other investigations (risk awareness, communication, allocation of responsibilities and duties)

   ➢ HR focused audits (remuneration, performance management)

   ➢ audits of risk management (credit risk strategy, risk appetite framework)

- **practical methodology** for complex risk assessment is missing or is not used

- Internal Audit has positive **influence** on risk culture :

   ➢ its own existence and planned audits – preventative measure

   ➢ actively by pointing out inappropriate behaviours, conflicts of interest and grey zones with missing responsibilities

   ➢ informal contacts with managers, top management

Several options available to assess Risk Culture

Management controls assessment (MCA)

► MCA rating given in addition to control environment (CE) rating
► Firms are using a range of factors
► Range of practice in formality, quality and use of MCAs

Embedded in the audit lifecycle

► Risk culture factors embedded in:
  ► Overall audit planning process
  ► Built into every audit
  ► Culture deeply embedded on internal audit methodologies, tools, reports
  ► Cultural findings evaluated, documented and reported

Innovative audit techniques

Culture risk assessment
Key drivers of behaviors & culture
Where inherent risk resides, e.g. tone from top, supervision and monitoring, policies & procedures, rewards & recognition

One-off culture audits
Thematic audits, e.g., "tone at the top," risk reporting
Deep dives on areas perceived to culturally high risk

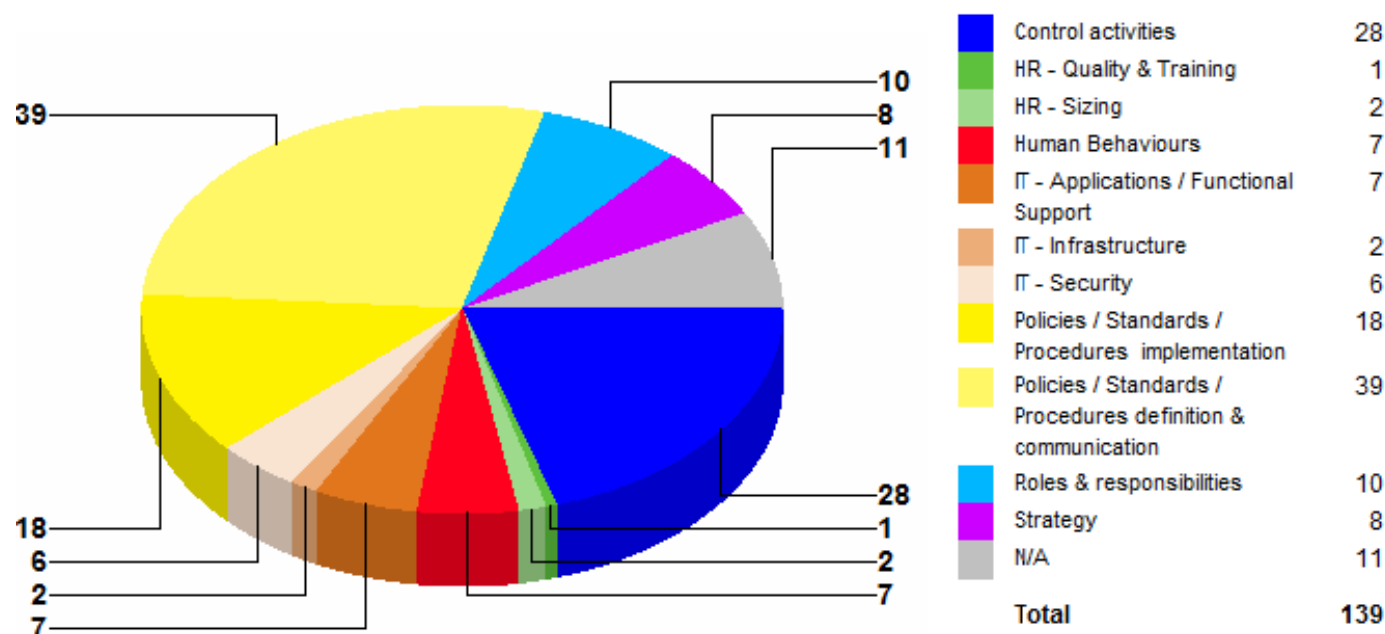# 2. Embedded in the audit lifecycle – risk culture factors built into audits

- **Define methodology for assessing risk culture elements in each audit by:**

  - ➢ **KPIs / generic work program / summary in audit report**

- **Easy to say** and define formally, **difficult to do**

- Provide a **way of thinking** for senior auditors rather than a mechanic audit test

- Attempt evaluation based on discussion with the audit team leader

	Element	Description of audit test
Example of possible audit checks	Tone from the top - Leading by example	Interviews with management incl. initial managerial risk self-assessment and its comparison against audit results - is management aware of key issues and proactively working towards addressing them?
	Tone from the top - Learning from past experience	Assess how information regarding emerging risks and control culture breakdowns are communicated bottom up to top management and how are they evaluated and what is done to improve
	Accountability - Ownership of risk	Assess the scope and design of managerial controls for their relevancy and adequacy. Select a sample of control results during the audited period and consider whether the controls were performed consistently and that the control results were properly evaluated and relevant actions taken focussing on non-routine controls involving judgement.
	Accountability - Escalation process	Obtain op risk events logged for the audited area and assess whether the causes have been sufficiently analysed, responsible employees identified and held accountable (e.g. warning issued / no bonus paid). Is there consistent approach to consequence management in time /across departments?
	Effective communication and challenge	Assess communication culture within the audited area: - are employees encouraged to raise concerns, ideas and discuss their views - is there sufficient informal communication between employees and managers so that employees can consult managers when needed - is there sufficient communication between business lines and between business and control functions
	Incentives - Remuneration and performance	Obtain MBOs for the audited area across all levels of management and for a sample of staff positions Review the goals and consider whether they are not conflicting with the position and encouraging excessive risk taking e.g. by high orientation towards profit. Consider how compliance aspects are built into the goals.

1

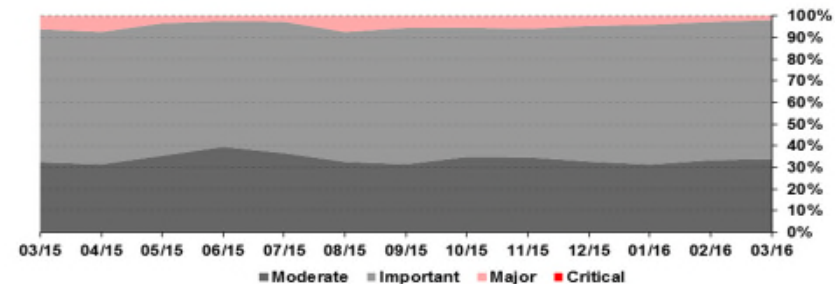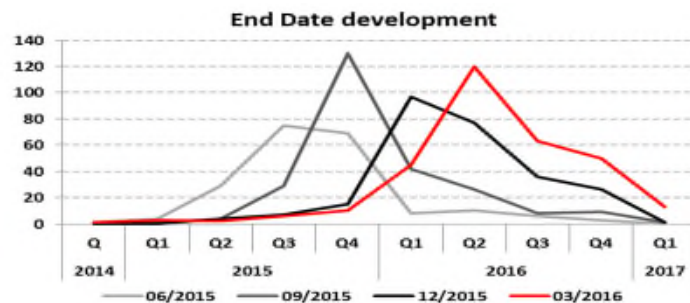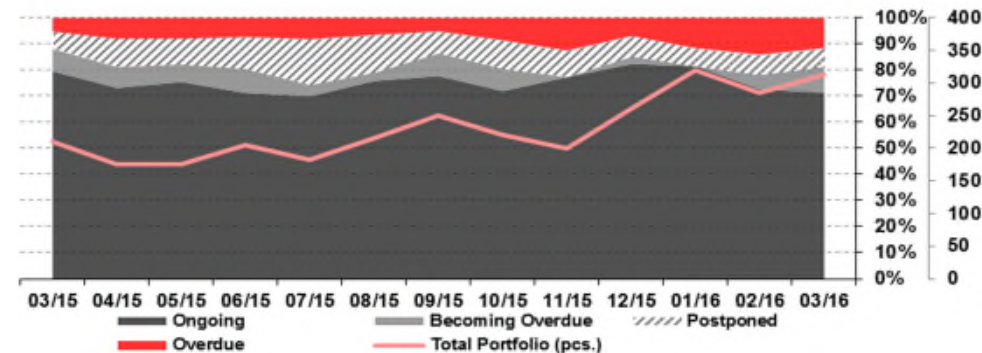# 2. Embedded in the audit lifecycle – root cause analysis

- Extract **root causes from audit findings relevant to risk culture** (for all findings with measures open or recently closed): eg control activities, behaviours, policies/standards/procedures implementation, policies/standards/procedures definition and communication, roles & responsibilities.

- Analyse the findings, remove those not relevant

- Analyse quantitative **trends** eg over time/YOY/in severity

- Analyse more in detail **high severity findings associated with risk culture**

Control activities	28
HR - Quality & Training	1
HR - Sizing	2
Human Behaviours	7
IT - Applications / Functional Support	7
IT - Infrastructure	2
IT - Security	6
Policies / Standards / Procedures implementation	18
Policies / Standards / Procedures definition & communication	39
Roles & responsibilities	10
Strategy	8
N/A	11
Total	**139**

2. Embedded in the audit lifecycle – tracking of audit measures

- Evaluation of risk culture can consist also of **trends** related to tracking of audit measures:

  - ➤ Population of overdue, postponed and becoming overdue measures

  - ➤ Average time to close Group Audit, External Auditors and Regulatory findings weighted by their severity

  - ➤ Results of second level controls testing (e.g. postponed/overdue measures)
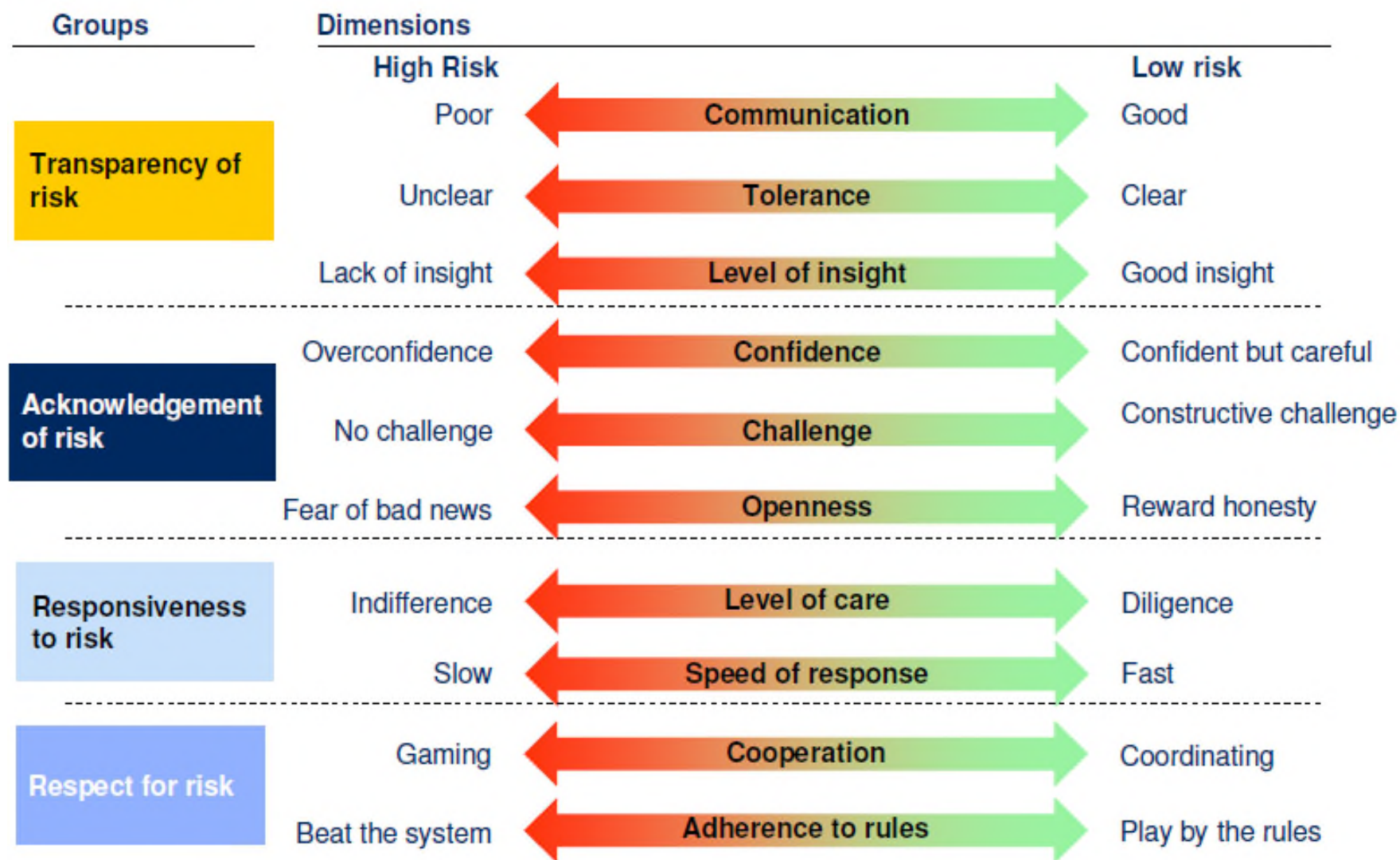
2. Embedded in the audit lifecycle – other sources of information

- **Consulting activities**: participation in key projects, internal rules/procedures review.

- Internal Controls Committee meetings, trends from the Ombudsman, regular meetings with key stakeholders (eg. COO, Head of OpRisk, Head of Compliance, Security).

- **Operational risk events**, risk limit, compliance and regulatory breaches – identify risk culture failures

- **Management** risk and control **assessment**

- Corporate events that can trigger **changes in risk culture**:

  - ➢ organizational changes, mergers and acquisitions

  - ➢ changes in key managerial positions

  - ➢ temporary changes due to significant projects

3. Innovative audit techniques

Risk culture framework

Groups	Dimensions	High Risk		Low risk
Transparency of risk	Communication	Poor	→	Good
	Tolerance	Unclear	→	Clear
	Level of insight	Lack of insight	→	Good insight
Acknowledgement of risk	Confidence	Overconfidence	→	Confident but careful
	Challenge	No challenge	→	Constructive challenge
	Openness	Fear of bad news	→	Reward honesty
Responsiveness to risk	Level of care	Indifference	→	Diligence
	Speed of response	Slow	→	Fast
Respect for risk	Cooperation	Gaming	→	Coordinating
	Adherence to rules	Beat the system	→	Play by the rules

3. Innovative audit techniques

- Culture risk assessment and one-off complex culture audits are extremely difficult to be performed with the skills, experience and resources of Internal Audit. Required skills include psychologists and HR specialists. In addition, insight and experience across several companies/industries is beneficial.

- In addition, there is often no sponsor for this huge exercise. However, corporate changes, history of failures or high inherent risk might trigger such demand and Internal Audit can definitely assist.
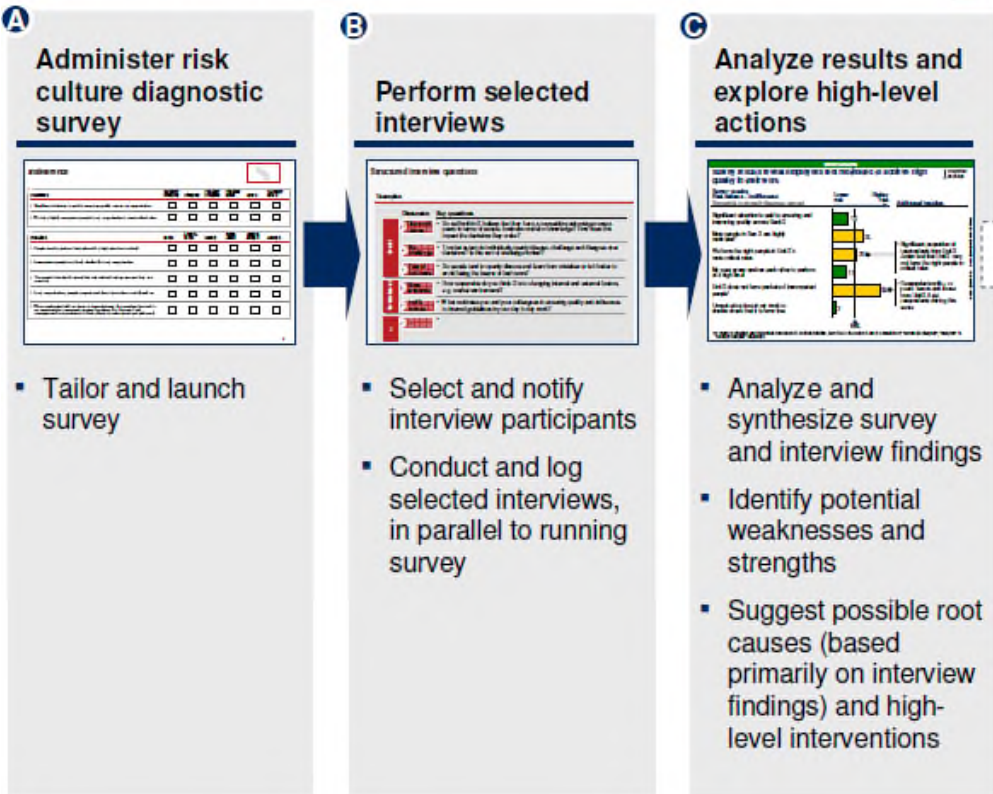
Where do we go from here?

■ It's not easy but it needs to be audited

■ Avoid formalistic approach where the subject matter is missing

■ Analyse well causes of corporate failures and audit findings – try reverse engineering to identify cultural factors

■ Watch behaviour of management and their subordinates

■ Speak about risk culture as part of each audit with the audit team

■ Try to gain interest of top management about risk culture assessment