Having a Risk Mindset

ISACA San Diego

March 17, 2022

Presenter

Meghana Jagdish
Director, Internal Audit
Illumina

Digital Heist Orchestrated by Former Microsoft Employee

What Happened:

A former Microsoft Software Engineer (V. Kvashuk) was **trusted** with "test-accounts" intended to inspect Microsoft's e-commerce operations

He decided to abuse the system and stole **$10M worth of gift cards** and sell them online

Much of the money was stolen **using test email accounts of other Microsoft employees**

Impact:

Kvashuk was flagged for suddenly being able to purchase a Tesla and $1.7M dollar home!

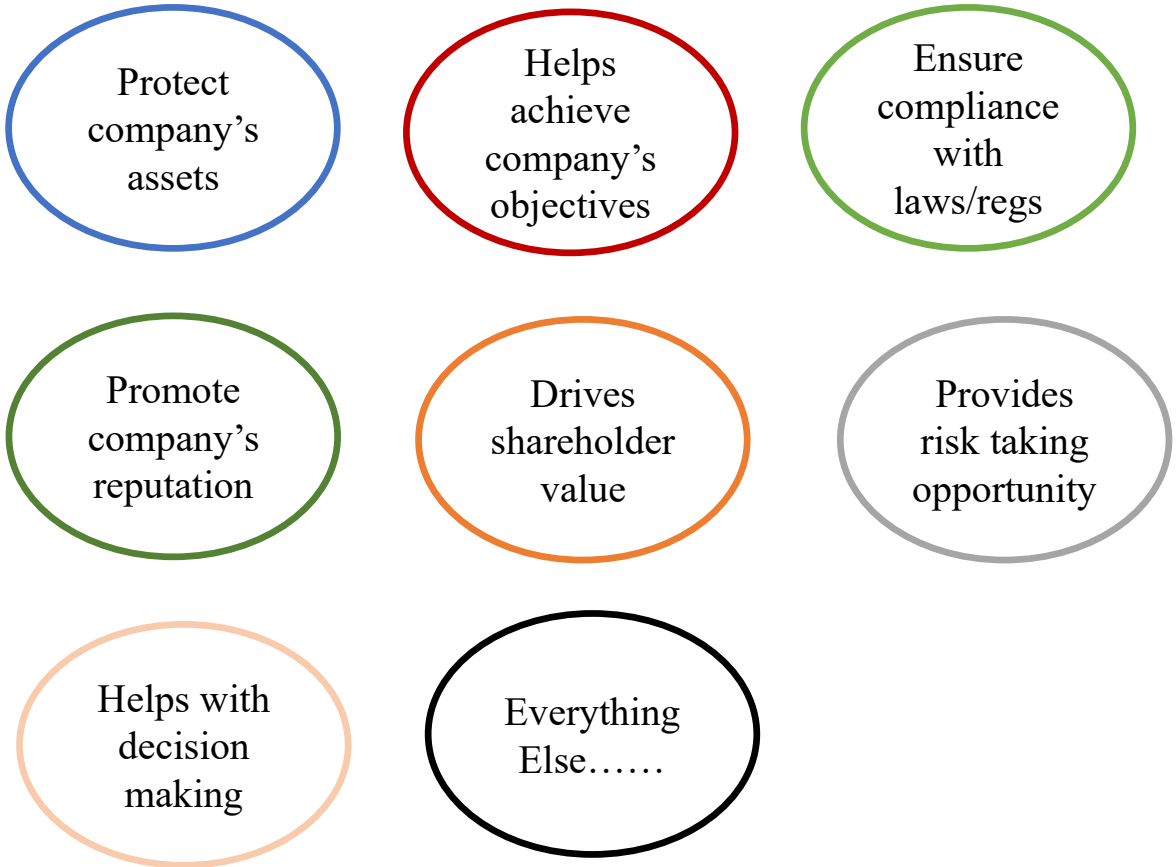
- Fired from Microsoft
- Sentenced to 9 years in prison and pay $8.3M fine
- He had used **accounts of other employees** to bypass suspicion, subjecting those employees to also being charged

Source: Fox News and Bloomberg

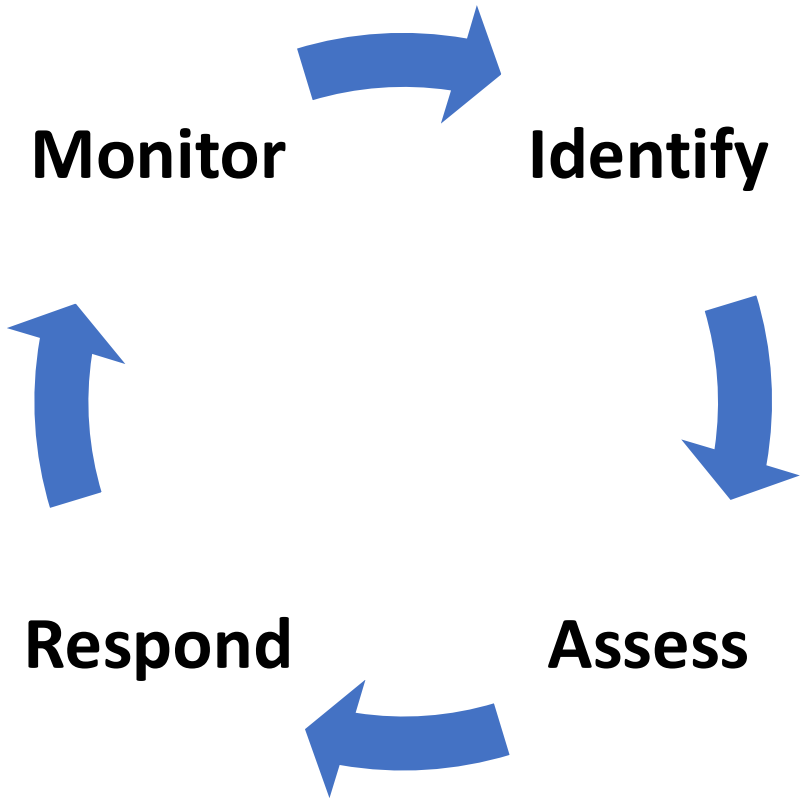
What is meant by Risk?

Risk is a threat that an event or action will affect the organization's ability to achieve its business objectives and strategies

Why is Risk Management Important?



Risk Management Process



Risk Management is an ongoing process, not a one-time event

Zoom Polling Question

What mechanisms do you use to identify risks?

A. Surveys or questionnaires

B. Periodic (e.g. annual) risk assessments

C. Table-top or simulation exercises

D. Vulnerability assessments

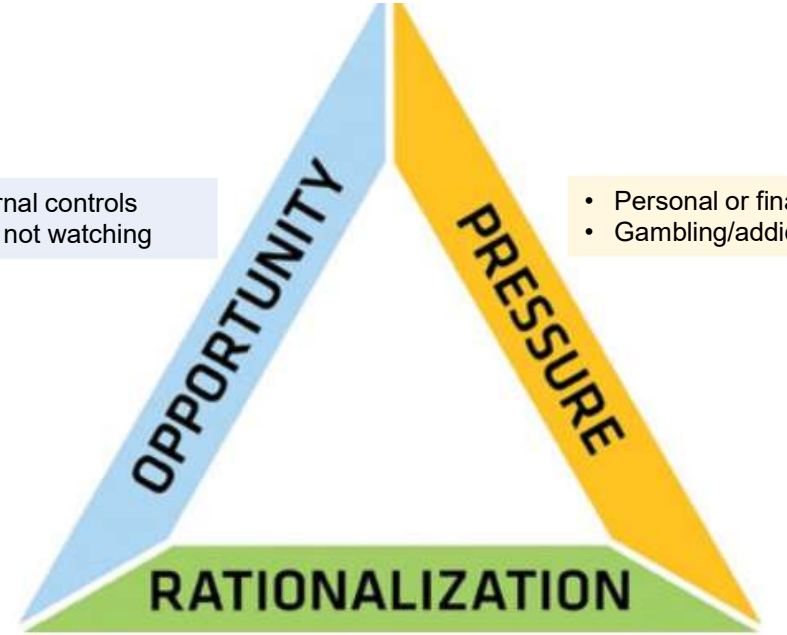
E. Other (please specify)

What are internal controls?

Actions taken to enhance the likelihood that established goals and objectives will be met (or reduce the likelihood of risk manifesting)

What happens when you ignore internal controls?

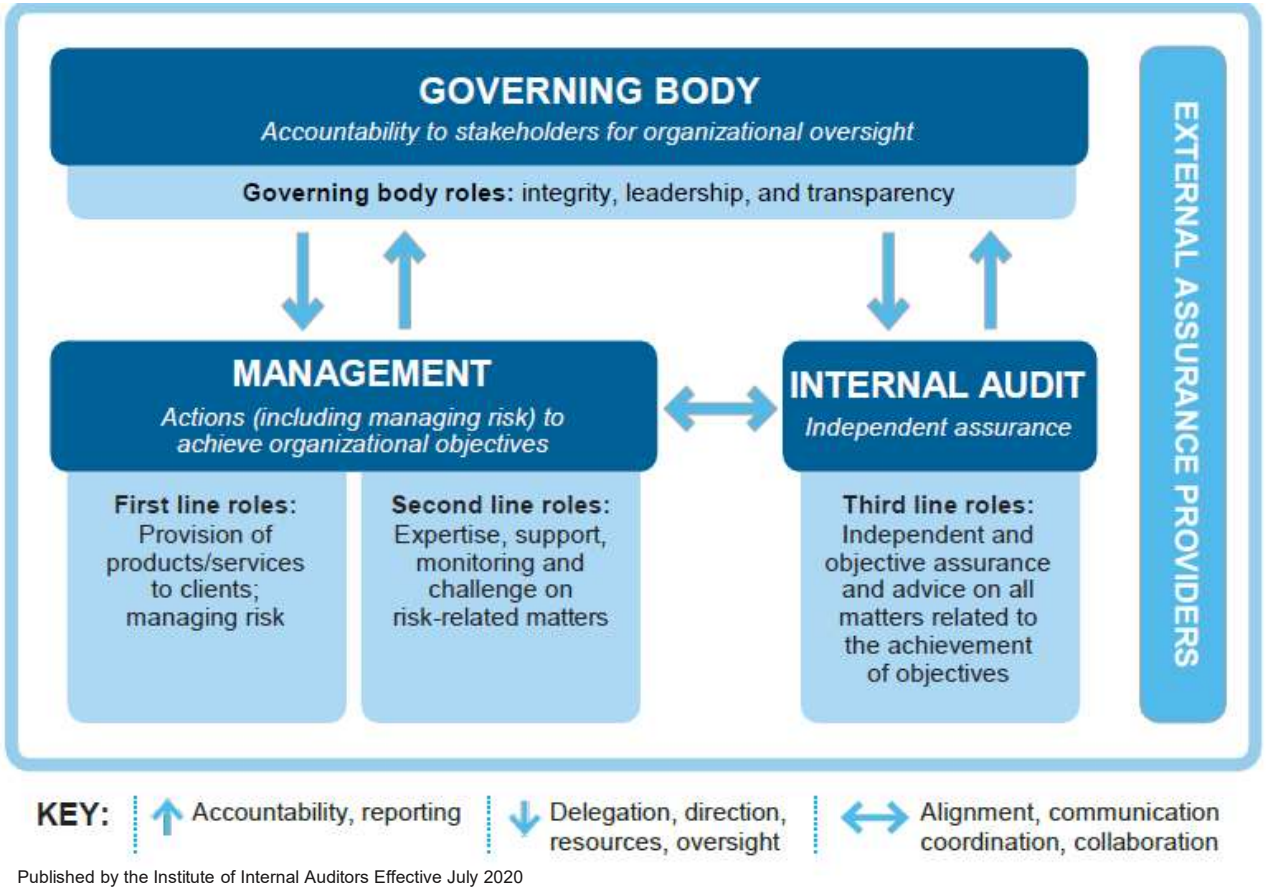
- Lack of or weak internal controls
- Senior management not watching



- Personal or financial pressures
- Gambling/addiction

- Justification of dishonest actions
- “It’s only a loan, I will pay it back”

Who is Responsible for Risk Management?



Published by the Institute of Internal Auditors Effective July 2020

Three Lines can work together to improve an organization's risk management structure

Wells Fargo – What happens when Three Lines Fail

What happened?

Employees boosted sales figures by covertly opening over 1.5 Million accounts and funding them from consumers' authorized accounts without their knowledge or consent

Where the Three Lines Failed?

- Wrong Tone at the Top
- Lack of accountability amongst sales org peers
- Corporate risk management didn’t identify the risks
- Material misstatements not identified as part of internal or external auditor testing

The cost of failure

- Impact to stock performance and about $1B in fines
- Had to make changes to its sales practices and internal oversight mechanism

Source: Forbes and IIA Blog

#Dieselgate

What happened?

Defeat device software was installed in cars to keep nitrogen oxide emission from diesel engines within legal limits during tests, while on road emissions were 40 times higher. This violated federal emission laws.

Where do you think the Three Lines Failed? – *Please use chat function*

- Lack of appropriate tone at the top
- Lack of accountability amongst engineering groups
- Inspection teams did not highlight this issue
- Quality auditors missed this design flaw

Source: BBC

How have risks evolved in these uncertain times?

- Cybersecurity
- Supply Chain Disruptions
- Talent Acquisition and Retention
- Inflation Pressures
- ESG/Climate Change

Robust risk management, especially in times of uncertainties, can help companies adapt and thrive

Zoom Polling Question

What other emerging risks do you see in the post COVID world?

A. Third Party Risk Management

B. Company Culture

C. Political Volatility

D. Regulatory Changes

E. Others (please specify)

IIA OnRisk2022 Risks

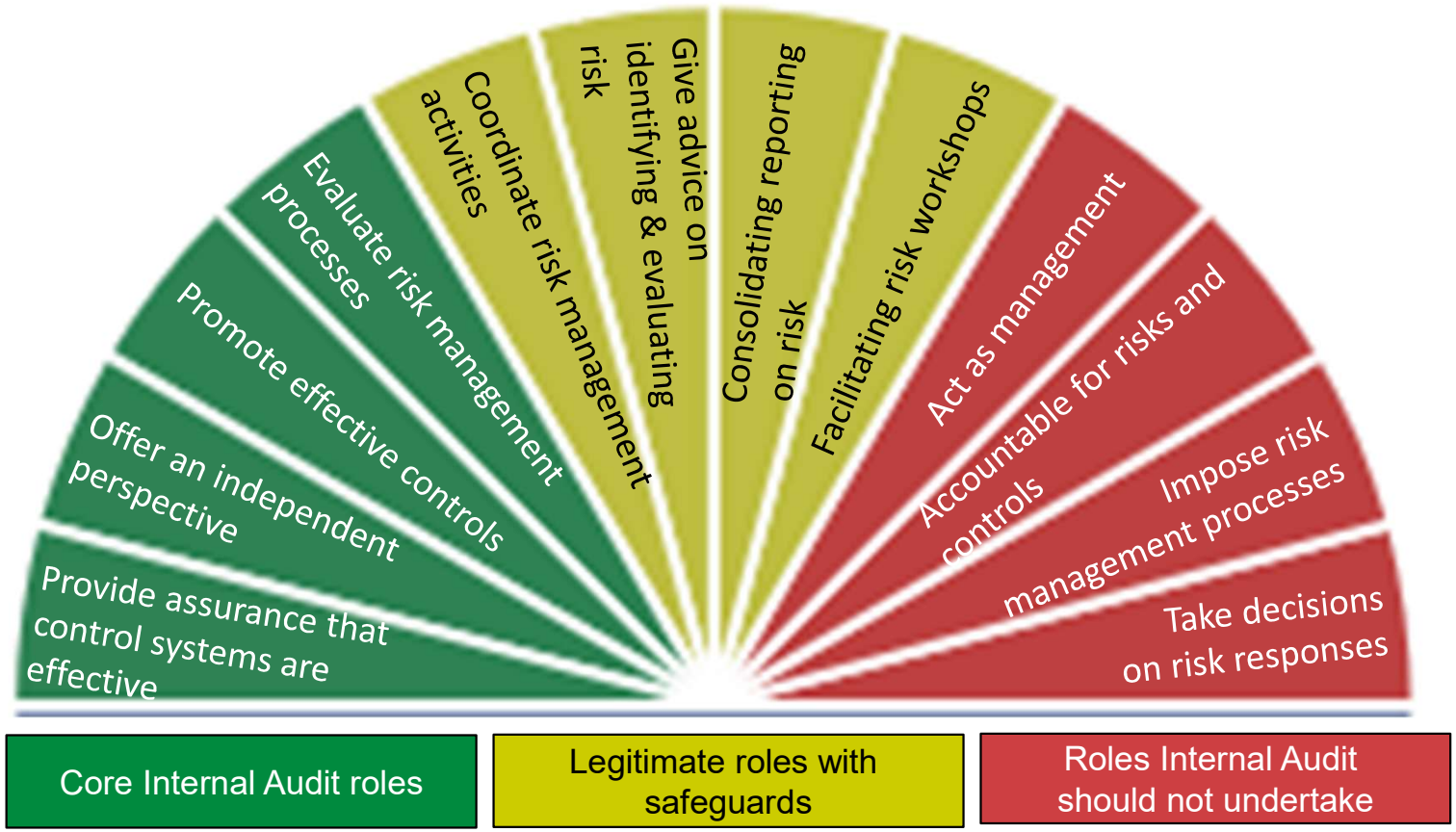
1. Cybersecurity
2. Talent Management
3. Organizational Governance
4. Data Privacy
5. Culture
6. Economic and Political Volatility
7. Change in Regulatory Environment
8. Supplier and Vendor Management
9. Disruptive Innovation
10. Social Sustainability
11. Supply Chain Disruption
12. Environmental Sustainability

Link: https://iia.no/wp-content/uploads/2021/10/2022-OnRisk-Report.pdf

How can you enhance the risk culture within your organization?

- Set the right Tone at the Top
- Educate the workforce….and apply skepticism
- Align on the guardrails (risk appetite)
- Think broader than financial risks
- Define measurable metrics (lagging and leading KRI/KPIs)

What Internal Audit Can and Can't do



Key Takeaways

- Identify risks and continue to monitor for changes in risk profile – especially as there are changes in people, processes and technology
- Coordination, alignment and communication between three lines is key to a positive risk culture – know your role!
- Risk management should be simple, real and easy to understand

Thank you!!!