hfma wisconsin chapter

Organizational Culture

And its relationship to Information Security and Compliance

1

hfma wisconsin chapter

Contents

- Introduction and background
- Definitions
- Procedures are not enough – a parable
- Parts of enterprise
- Warning signs
- Elements of an effective culture
- Open discussions
- What you can do

2

hfma wisconsin chapter

Introduction and Background

What are the conceit and assumptions for this presentation?

Learning objectives

Why is this important to this audience?

3

hfma wisconsin chapter

The Conceit and Assumptions

- Information security and compliance with relevant security regulations are technical problems
  - Assumption 1 – It is all about policies, procedures and controls
  - Assumption 2 – It is an operational management-level problem, not strategic in nature
  - Assumption 3 – These processes can be managed in silos
  - Assumption 4 – Sales, Finance, Clinical, Billing, Customer Service and Board have bigger fish to fry
  - Assumption 5 – People will do the right things

4

hfma wisconsin chapter

Learning Objectives

1. Information security and compliance is not solely the responsibility of technical teams or compliance personnel.
2. There can be positive and negative aspects of an organization's culture that can have pervasive impacts on both control design and effectiveness.
3. Finally, other organizational initiatives and incentives may impact, or be impacted, by the information security controls and compliance activities.

5

hfma wisconsin chapter

Why is this important to me?

Derived from *What Finance Leaders Should Know About Cybersecurity Risks*, Hegwer, Laura Ramos. May 31, 2017 HFMA.org

6

hfma wisconsin chapter

Definitions

Corporate/organizational culture, information security and compliance

7

hfma wisconsin chapter

What is Organizational Culture?

- Definition of Culture
  - The way we do business around here (behaviors)
  - Who and what we focus on and spend resources on (values)
- How you can tell it is genuine
  - Leadership interactions
  - Crises
  - Tough decisions and easy outs

8

hfma wisconsin chapter

Information Security

- Information security is managing risks to the confidentiality, integrity and availability of information using administrative, physical and technical controls[1]

1 Francen, Evan *Unsecurity*, Beaver's Pond Press, Minneapolis, MN 2019

9

hfma wisconsin chapter

Compliance

- Compliance is the act or process of complying to a desire, demand, proposal, regimen or coercion; it is conformity in fulfilling official requirements[2]

2 IBID

10

hfma wisconsin chapter

Procedures are not enough – a parable

Parables from my experiences with Total Quality Management, Six Sigma, Statistical Process Controls, ISO-9000, etc.

11

hfma wisconsin chapter

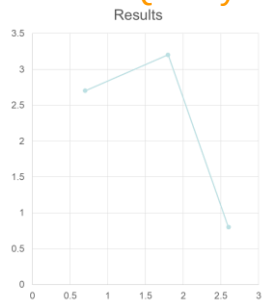
Quality Revolution!

- By the late 1970s, it was obvious that U.S. manufacturers had quality issues!
- Deming, Juran, Crosby, Baldridge, et al
- Beginning in 1984 I was immersed this stuff

12

hfma wisconsin chapter

Quality Revolution!



- TOOLS - MANAGE THE PROCESS
  - SPC
  - Scientific Management
  - Process Re-Engineering
  - Six Sigma

13

hfma wisconsin chapter

Quality Revolution!

- METHODS - MANAGE THE PEOPLE
  - Quality Circles
  - T-shirts
  - Parties
  - Union Contracts

14

hfma wisconsin chapter

Quality Revolution!

- MATERIALS - Standards and Policies
  - ISO 9000
  - QS 9000
  - Q1
  - Policies (many trees gave their life…)

15

hfma wisconsin chapter

16

hfma wisconsin chapter

Health Care Information Security

- We have got tools (anti-malware, firewalls, G.R.C, S.I.E.M, vulnerability scanners, etc.)
- We got the methods (training and awareness, CISO position, chief compliance officers)
- We got the materials (HIPAA, NIST, PCI, COBIT, etc.)

17

hfma wisconsin chapter

All it Takes…

- One misguided management decision can and has killed all of the motivation and efforts put into a program
  - Or
- Hiring, retaining or promoting individuals who do not buy in with the program

18

hfma wisconsin chapter

Lessons Learned

- Success of the initiative is dependent upon everyone being aligned
- You get one chance to make a first impression!
- You may not like what happens
- Run the play that is called
- Walk the walk
- Crises or urgency is not an excuse to bypass the agreed-upon procedures
- Build and communicate exceptions

19

hfma wisconsin chapter

Parts of an Enterprise

Information Security and Compliance are not operating in a vacuum

20

hfma wisconsin chapter

Enterprise Impacts

- Impacts of IS and Compliance to Enterprise
- Enterprise Initiatives Impacts to IS and Compliance

21

hfma wisconsin chapter

Impacts of IS and Compliance

- Constraints on business opportunities and programs
- Costs to all IS and Compliance activities
- Resources
- Impacts and requirements need to be integrated into the business plan models

22

hfma wisconsin chapter

Enterprise Initiatives Impacts

- Process and controls may change
- Introduces new risks
- May require new procedures
- Resource constraints

23

hfma wisconsin chapter

Warning Signs

How do you know if you have a culture problem?

24

hfma wisconsin chapter

Possible Warning Signs

- No seat at the table
- The “No” folks
- Long running issues
- Ignorance of risks
- Lack of actionable plans
- Repeat offenders go uncorrected
- High turnover

25

hfma wisconsin chapter

Possible Warning Signs

- Excessive exceptions to the rules
- Suspended in times of crises or higher priorities
- “Do it because I said so”
- F.U.D.
- External findings
- Lack of resources
- Little or no security and compliance metrics

26

hfma wisconsin chapter

Components of Good Culture

What are some key attributes of safe, responsive and viable culture that support information security and compliance?[3]

3 Coyle, Daniel *The Culture Code: The Secrets of Highly Successful Groups*, Bantam Books, USA 2018

27

hfma wisconsin chapter

Make it safe

- Spotlight your own fallibility
- Embrace the messenger
- Overdo thank-yous
- Be painstaking in the hiring practice
- Eliminate bad apples
- Make sure everyone has a voice
- Pick up the trash

28

hfma wisconsin chapter

Share vulnerability

- Make sure the leader is vulnerable first and often
- Over-communicate expectations
- Deliver the negative stuff in person
- Aim for candor, avoid brutal honesty
- Align language with action

29

hfma wisconsin chapter

Establish purpose

- 10 X as clear about your priorities
- Embrace the use of catchphrases
- Measure what really matters
- Use artifacts
- Focus on bar-setting behaviors

30

hfma wisconsin chapter

Open Discussions and Questions

Questions and discussions

31

hfma wisconsin chapter

Group Discussions

1. How do you think that the combination of culture and controls can affect the risk of fraud, waste and abuse (based upon the fraud triangle)?
2. What is the risk of an overly restrictive or punitive culture in relation to maintaining information security, incident management and compliance?
3. What is the risk of an overly liberal or lax culture in managing security and compliance events?
4. What can organizations do to balance the need for innovation or speed in the market and ensuring security and compliance?

32

hfma wisconsin chapter

Things Finance Leaders Can Do

1. Identify, prioritize and safeguard crucial data
2. Support the investment in using a risk-based cybersecurity framework
3. Support investment in cybersecurity insurance
4. Review the data breach response plan
5. Collect and analyze security risk reports on a periodic basis
6. TAKE THE LEAD TO DEVELOP A CULTURE OF CYBERSECURITY

4 Derived from Parikh, Chetan. The Finance Leader's Role in Cybersecurity, HFMA.org, October 9, 2017

33

hfma
wisconsin chapter

Charles Snyder
BKD Cyber
csnyder@bkd.com
Office: 502.581.0435
Mobile: 502.419.2931
bkdcyber.com

34