Theory vs Reality in your Policies and Procedures - the Dangers of Aspirational Compliance

- Janet Himmelreich, Managing Director, 3Comply

- SCCE Philadelphia Conference, Dec. 6, 2019

1

Discussion Items

- Policy vs. Procedures
- Other Types of Documents
- Do You Practice Aspirational Compliance?
- What Is Aspirational Compliance Anyway?
- Case Study
- Things You Can Do Back At the Office

2

P&Ps

Define:

Policies

Procedures

Processes

How different from P&P?

Where and when used?

Using these terms interchangeably is confusing

Policies vs Procedures

Policies

- Rules behind what is going on – including regulations
- The "What" and "Why"
- Provides a framework PM1
- Answers the question – would I fire you?

Procedures

- How you meet requirements; Who, when, where is addressed
- Operational Groups often formulate
- Day to day activities
- Enforce consistency PM2
- Tie to policies

Slide 4

PM1 and a discipline
Pascal Marat, 11/21/2019

PM2 Create visibility and
Pascal Marat, 11/21/2019

Other Types of Documents

- Guidelines
- Playbooks
- Work Instructions
- Processes
- Strategy
- Plans
- Assessments

- "documents" may be inside an automated process; solely kept electronically etc.
  - Advantages
  - Disadvantages

Do You Practice Aspirational Compliance?

Considerations:

- Items that reside in policies and procedures (and perhaps elsewhere) that are things that:
  - Someone *thinks* should be done
  - Someone *wants* to be done
  - Someone *heard* should be done or would be happening "soon"
  - Someone *believes* IS the way it is being done
- Who wrote the P&Ps?
- Have you had a recent change in leadership? Change in strategy? Has a new law come into effect? Were you or a competitor or sister company fined for something?

So, do you practice aspirational compliance?

P&Ps and Aspirational Compliance

- Case study –
  - Background: company has a handful of HR related policies, automated processes reflected in systems used for business (not written separately) and a very long "Security Policy" that mixes policy statements, tasks and steps as well as processes and procedures
  - A review of the Security Policy reveals:
    - Statements regarding the position the company takes relative to security of customer data, employee data and Privacy in general
    - How to reset a password
    - Steps to request and receive an exception to the policy
    - The values the company is protecting by having the policy
    - Technical security solutions today and planned
    - Directions as to how to make determinations of classifications of risk including things planned

7

Dissection of study

What problems do you see?

How would you approach revisions?

What might contain aspects of aspirational compliance?

8

The Dangers of Aspirational Compliance

- Overstatement
- Creating obligations
- Writing things down that require funding which is not in place
- Failing audit or assessment (can be internal or external)
  - Fines
  - Remedial activities
  - Loss of accreditation/certification/approval
  - Breaking contract obligations
- Others?

Back at the office

- Check who the author(s) were
- When were documents last reviewed? Is that record up to date? Including in systems.
- Were documents that should have been retired actually retired?
- How do you classify documents?
- Look for things written down you don't or can't do
- If templates were used, were they appropriate for the content?

The $64k question…

If you were audited against your policies and procedures would you be able to evidence that you follow them (precisely)??

About 3Comply

3Comply believes that most people hate compliance because it is too complicated, expensive, and threatening. We believe that you can "Comply Simply". We bring a collective 70+ years of compliance experience to guide our clients in the best ways to integrate compliance into normal business operations.

3Comply is a principal owned and managed Compliance Advisory Services firm. Our services are built around Regulatory Compliance, Privacy and Cybersecurity Governance.

From multinationals to startups, we can help you establish the right level of compliance program to "*Comply Simply"*.

Check us out at www.3Comply.com

Contact Janet directly at Janet.himmelreich@3Comply.com