



Designing a Compliance and Governance Model for Today's Hi-Tech Business Environment

Annual Compliance & Ethics Institute | Gaylord National | National Harbor, MD
September 18, 2019
10:15 – 11:45am

1



PRESENTED BY OPTUM COMPLIANCE TEAM:

Eric Brotten, @ebrotten
Director
Compliance



Sarah Boswell-Healey
Director
Privacy Compliance

2

Today's Presentation

- Evolution of Technology and Compliance Implications
- Building Blocks and Support Methods
- Lessons Learned
- Break-out and Group Discussion
- Q&A

3

Audience Survey Question #1

What industry are you in?

- A. Financial services / Banking
- B. Pharma /Healthcare /Med. Device
- C. Food services /Food production
- D. Energy /Oil /Gas
- E. Manufacturing
- F. Automotive
- G. Other

4

Audience Survey Question #2

Do you work for a tech company?

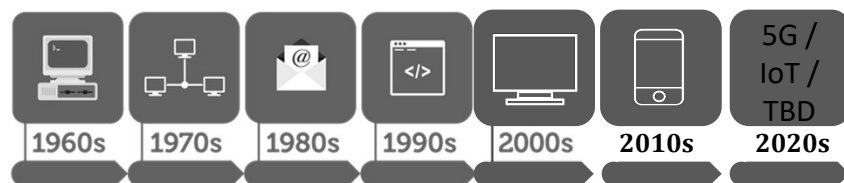
A. Yes

B. No

5

Evolution of Technology

Example: Internet



Source: <https://online.jefferson.edu/communications/internet-history-timeline/>

6

Evolution of Technology

Example: Mobile Phone

1980s – multifunctional tool: could be used as a phone, doorstop or weapon.



2019 – multifunctional tool: could be used as a phone, computer, a thermostat for your home, medical device?

7

Evolution of Technology

Example: Healthcare

1980s – Pre-HIPAA;
Documentation in Paper;
illegible Scripts filled at
bricks and mortar
Pharmacy



2019 – State, Federal, and International layered IT Security, Data Governance and Privacy requirements; electronic documentation; Home Delivery Pharmacy managed through your smart phone

8

Evolution of Technology

“Every company is now a technology company”

(Christopher Mims, The Wall Street Journal, Dec. 4, 2018)



9

Audience Survey Question #3

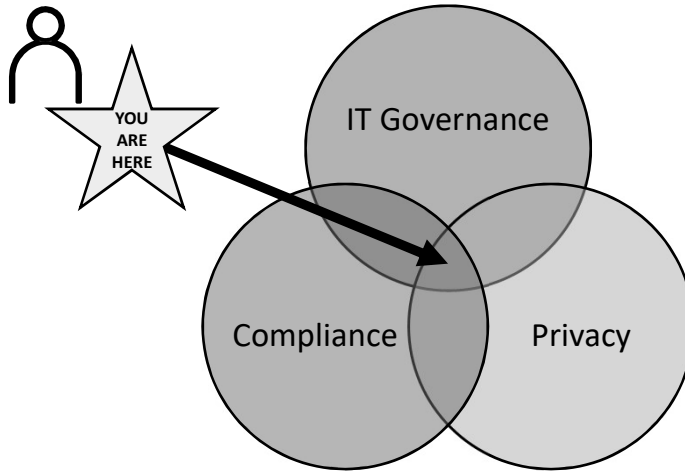
Again, do you work for a tech company?

A. Yes

B. No

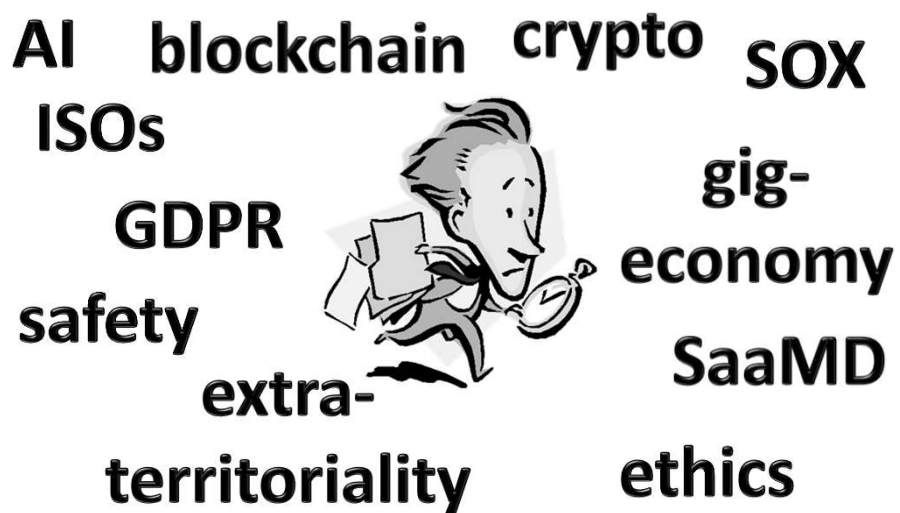
10

Evolution of Technology:
What Does It Mean For
Today's Compliance Professionals?



11

Evolution of Technology:
What Does It Mean For Today's Regulators?



12

Today's Compliance Favors Diverse Work Experiences

Eric: Business/IT Product

Sarah: Museum/Waitress



13

Today's Compliance Favors Cross-Functional Teamwork



14

Audience Survey Question #4

I know and understand how my business partners run their projects within agile and waterfall frameworks.

- A. True
- B. False
- C. What the heck are agile and waterfall?

15

Product / Project / Service Delivery Development Methodology

Traditional Waterfall



- Sequential
- No back stepping
- Initial extensive plan must be followed, or entire project scrapped

16

Advantages for the Compliance Practitioner

Traditional Waterfall



- Lots of upfront and on-going record/progress keeping
- You know what to expect
- Easy to assess risks, even without team assistance/cooperation (due to heavy documentation)

17

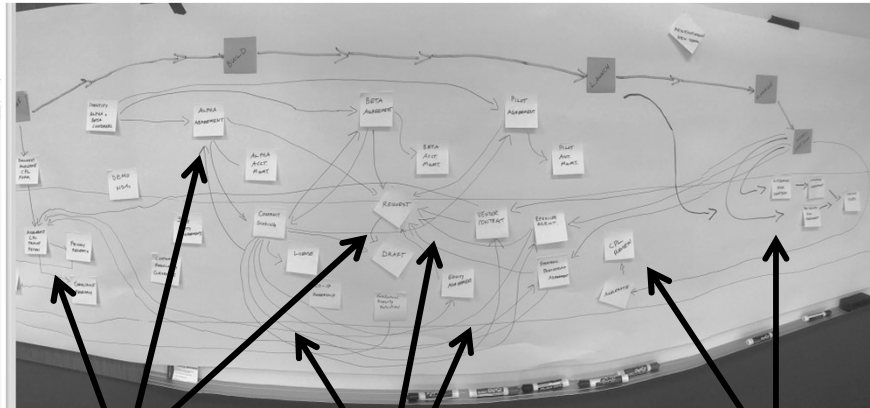
Waterfall Development: Why change a good thing? (for a compliance practitioner)

- No re-do's
- Bugs / errors
- Inflexible
- Speed to market slow (only when project done)



18

Think You Don't Need to Learn Agile?



EXTRA STEPS

REWORK

WASTE

The business impact of a non-agile friendly compliance practitioner.

23

Building Blocks of Agile Terminology

- **Sprint(s):** A small package of work typically worked on weekly or monthly schedules. At the end of each “sprint” the project is re-evaluated and tested.
- **Scrum/Agile Team:** A multi-disciplinary team tasked with completing the sprint.
- **Scrum Master:** The scrum team facilitator, coach, and roadblock remover. Typically hosts a daily “scrum” meeting with team and manages the sprint cycle.
- **Scrum of Scrum:** In projects with multiple sprints, a forum where Scrum Masters collaboratively issue spot and coordinated the overall delivery.

24

Building Blocks of Agile Terminology (cont.)

- **Roadmap:** The high-level vision, plan, and strategy to achieve the desired results.
- **Backlog:** A catalog of features or project elements that are needed to drive the roadmap forward and continuously prioritized.
- **Delivery System:** The overall agile system of strategy, program management, delivery and release.
- **Feedback Loop:** The mechanism (or forum) in which the project or product is continually evaluated against expectations and requirements (internal testing, pilots/betas, customer feedback, etc.)
- **Deployment/Release:** The point when the product or project has enough “meat” to be launched, set-off, or commenced.

25

Building Blocks of Agile Terminology : Common Development Phases

- **Ideate:** The project or product is brainstormed by the program team.
- **Define:** The idea (project or product) is placed into a set of parameters or scope.
- **Build:** The project or product is developed against the scope.
- **Launch:** The project or product goes “live” and is delivered to a customer, partner, etc.
- **Manage:** The live project or product is evaluated and re-evaluated against expectations and/or new requirements.

26

Audience Survey Question #5

Which companies use agile methodologies in their product and service delivery?

- A. 3M
- B. IBM
- C. Australia and New Zealand Banking
- D. Google
- E. Spotify
- F. Monsanto
- G. All
- H. None

Sources:

<https://www.quickstart.com/blog/how-agile-scrum-training-transformed-these-5-companies/>
<https://www.datascience.com/blog/inside-monsantos-digital-transformation>

27

Getting Ready to Implement an “Agile” Compliance and Governance Model

Before you jump into your business’s agile delivery system, you must make your own compliance and governance team “agile”



28

The Transformation to Agile Compliance and Governance



- Accept that your business partners will change their minds and course constantly
- Be solution-focused, not “Dr. No”
- Acknowledge the blurring lines across compliance, privacy, and legal practitioners
 - Cross-train on areas of subject matter expertise
 - Avoid burnout and use shared coverage of business agile delivery for issue spotting
 - Hold your own internal ‘scrum’ sessions

29

Implementing an Agile Compliance and Governance Support Model

Remember this? Agile

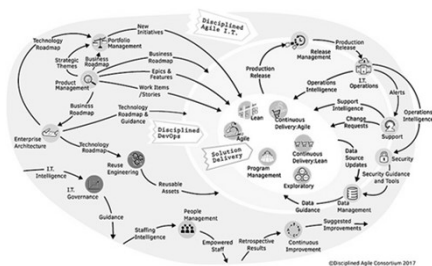
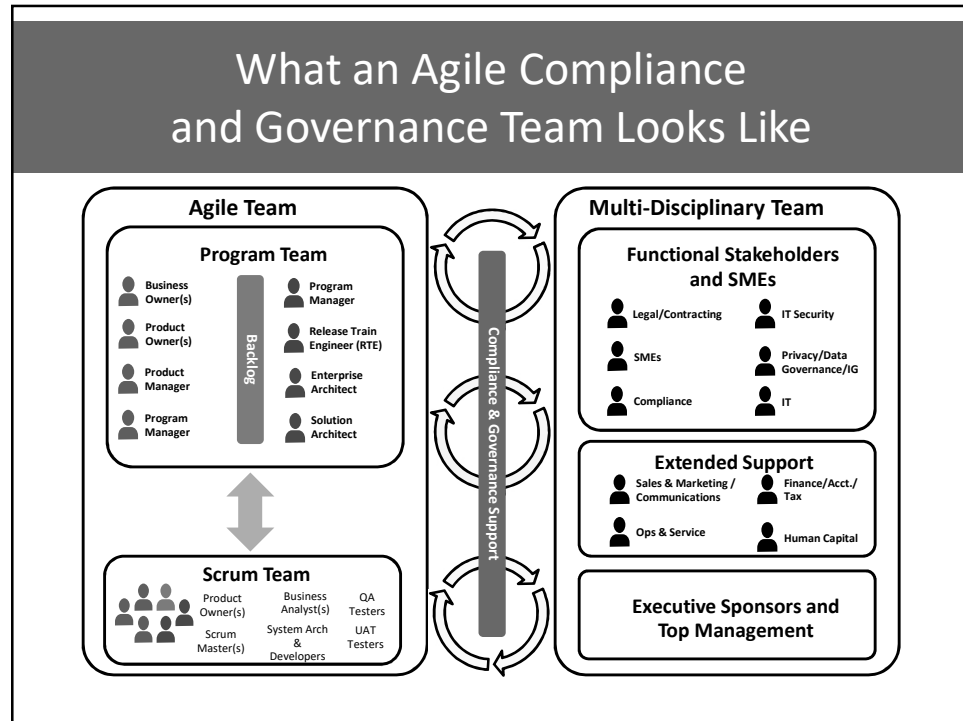


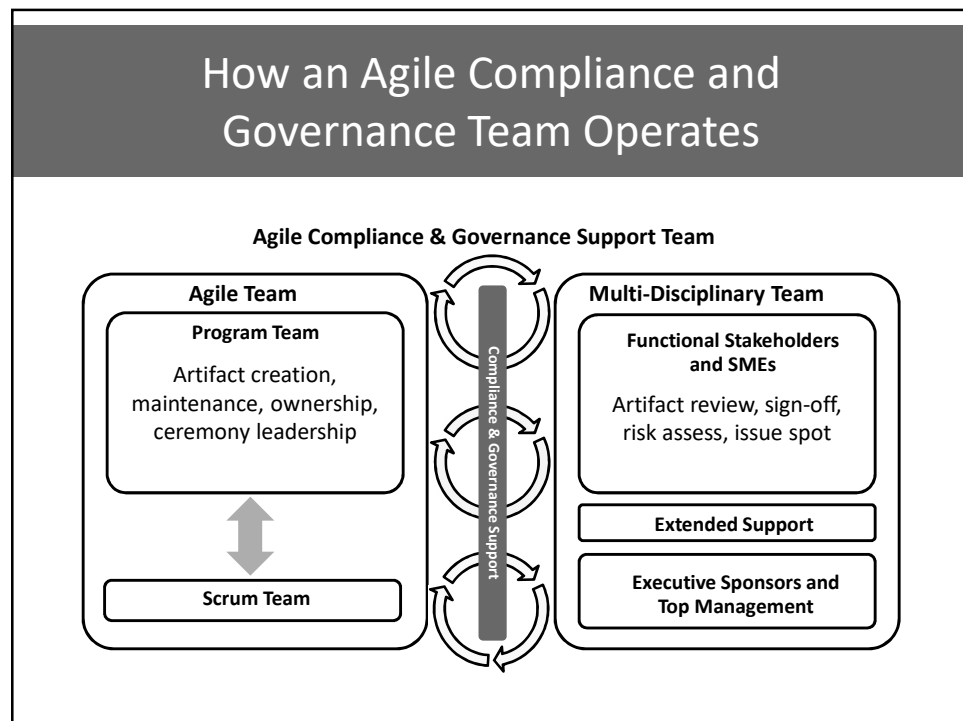
Image source: <http://disciplinedagiledelivery.com/agility-at-scale/disciplined-agile-2/>

- Meet your business where they are, i.e. embed yourself in the agile delivery - EARLY
- Provide continuous and on-going advisory support
- Prevent waterfall bombs, e.g. “I didn’t know you were doing that! You can’t do that!!!”

30



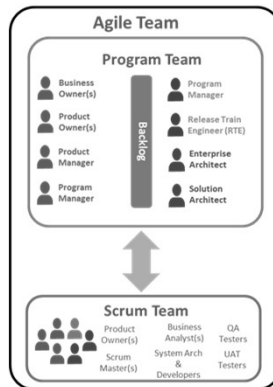
31



32

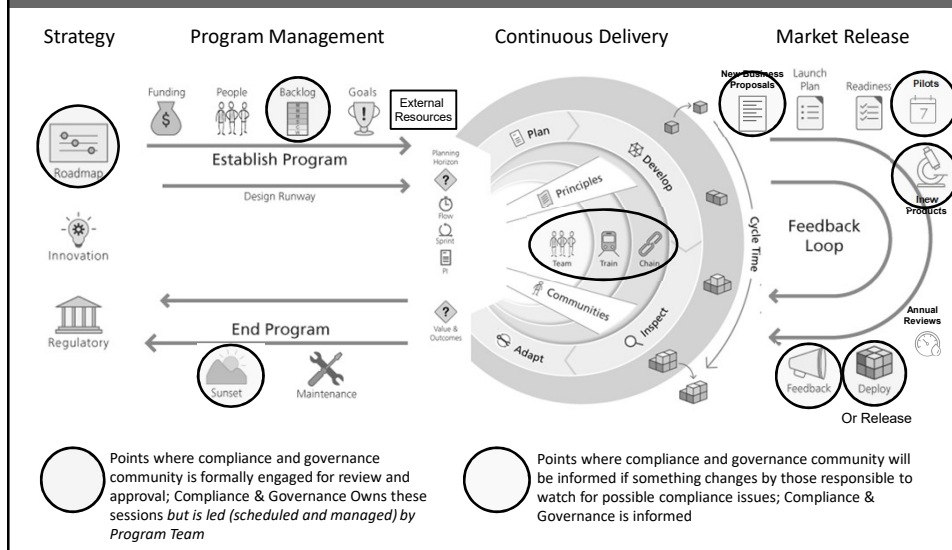
Bonus Round 1

Within an Agile Team, who are the most important individuals for compliance and governance professionals to have a relationship with, and why?








33

Embedding Compliance and Governance into the Agile Delivery System



34






Agile Phase Descriptions

 Roadmap	 Backlog	 Delivery System	 Feedback	 Deploy / Release & Sunset
<p>The roadmap offers high level visibility as to what the business is looking to develop and bring to market. The roadmap in an Agile context focuses on the next 3 to 9 months with an expectation that the 3 month vision is more accurate than 9 months down the road</p> <p>Meetings:</p> <ul style="list-style-type: none"> Road mapping Sessions 	<p>The Roadmap is translated into capabilities and features that offer just enough detail to allow solutions to be proposed and placed in the Program Backlog. The solution will be presented to the Product Management Council and Compliance and Governance Team for review and approval. This is the key governance phase.</p> <p>Meetings:</p> <ul style="list-style-type: none"> Project Management Council (PMC) Feature Refinement IGC Review 	<p>Agile delivery can be executed using a variety of methods. Regardless of the method, all of these processes have predictable, repeatable and reliable practices that will allow for compliance and governance to be embedded within each method. While already approved at the Feature backlog level, the delivery team will include a will know when to flag a User Story solution for review by Compliance and Governance Community.</p>	<p>Regardless of how the feedback may come; via the Help desk, account managers, or if it's an enhancement or defect, all changes to the product will go through either the O&M process or normal backlog process through the Delivery System. The Compliance and Governance Community will know if any new work or changes require their review.</p>	<p>Once our products and services are deployed this process allows us to have the confidence that our products and services in the live environment are both the best and complainant.</p> <p>In the event a product or service is scheduled to be sunset, the Compliance and Governance community will come together to ensure the entire process or sun setting and required artifacts are compliant.</p>

35

35

IT Security Compliance Requirements Within Agile

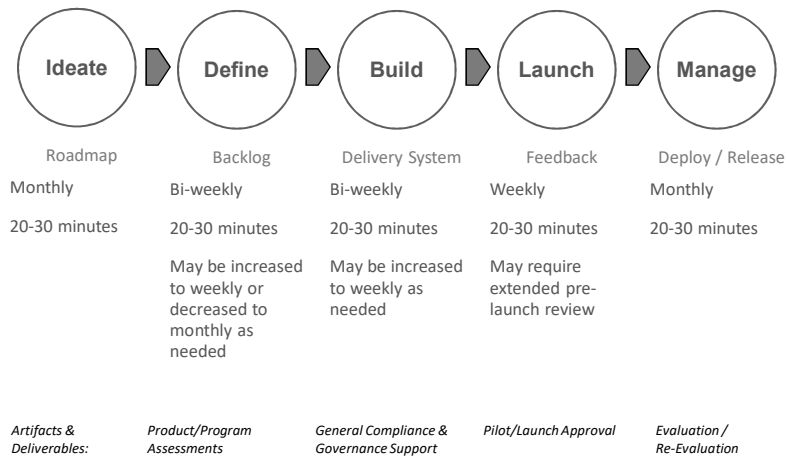
 Roadmap	 Backlog	 Delivery System	 Feedback	 Deploy / Release / Sunset
<ol style="list-style-type: none"> Identify MVP IG/ ITSEC requirements for product based on emerging in-region market requirements Align business product roadmap with security architecture strategy identifying critical path items and gaps Utilize control portfolio to identify Secure DevOps Gaps 	<ol style="list-style-type: none"> Delivery team to identify Capabilities that require security engineering of new patterns IG team sets clear definitions of done and acceptance criteria for key security capabilities (Eg: Authentication, SCA,) 	<ol style="list-style-type: none"> Delivery team must establish scorecard of quality of delivery through SecDevOps processes Delivery team to utilize design patterns for security controls, or create new patterns Perform Security Architecture reviews Security & Safety Champion will be established for each SCRUM team 	<ol style="list-style-type: none"> Program Increments will demonstrate compliance and security functionality Secure DevOps will enforce DoD and AC defined for security, feedback given through scorecard review 	<ol style="list-style-type: none"> Operational Readiness will ensure documented procedures for controls Delivery team will report on security testing and compliance

36

36

Compliance and Governance Cadence within the Agile Delivery System

Team meeting pace recommended for products/programs according to the following development cycle phase:



37

Bonus Round 2

Within agile delivery projects, what phase is most important for the compliance professional to get involved and get 'in the know'? Why?



38

Artifacts & Tools for Success: Roles & Responsibilities (RACI)

Multi-Disciplinary Role	Person	Compliance & Governance Attendance	Responsibility
IG (Privacy & Security)	Name 1	Required	<ul style="list-style-type: none"> General information/data governance and privacy SME / responsibility Review of privacy artifacts (data flow oversight) Approval of privacy artifacts Engagement with Privacy Legal as-needed Ensure IT Security standards and requirements are met
Compliance	Name 2	Required	<ul style="list-style-type: none"> General compliance SME / responsibility Review of compliance artifacts Approval of compliance artifacts Annual product/project compliance risk assessment
Legal and Legal Contracting	Name 3	Optional	<ul style="list-style-type: none"> General business legal SME / responsibility Engage legal contracting as required Identifies and manages customer agreement barriers to innovation
Extended Support	Name 4	Optional	<ul style="list-style-type: none"> IT / Platform SMEs Sales & Marketing Finance and Accounting Operations and Service Human Capital
Industry Specific SME	Name 5	Required	<ul style="list-style-type: none"> Certain industries may have varying needs for specific expertise, e.g. healthcare, energy, finance, bio tech, med. device, etc.

39

Artifacts & Tools for Success: Roles & Responsibilities (RACI) (cont.)

Role	Compliance & Governance Attendance	Project 1	Project 2	Project 3	Other
Senior Leadership	Optional				
Business Owner	Required				
Product Owner(s) (Traditional) Product Manager(s) (Agile)	Required				
Product Manager(s) (Traditional) Product Owner(s) (Agile)	Required				
Program Manager	Optional				
Agile Delivery (RTE)	Optional				
Solution Architect	Required				
Scrum Master	Optional				

40

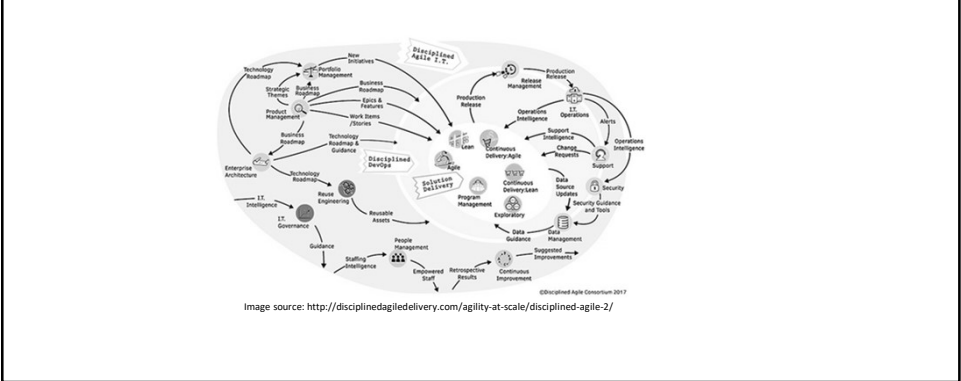
Other Compliance Artifacts & Tools for Success

- Incident Log
- Safety Reports
- Marketing Materials Review / Guidelines
- Privacy Compliance Documentation, i.e. data flows, data processing documentation, DPIAs, etc.
- Product Assessment Documentation
- Project Plans and Delivery Timelines
- Customer Contract Compliance Requirements Table and Template Language

43

Bonus Round 3

What is one thing you can do now to start implementing a more agile compliance and governance model?



44

Other Tips and Considerations

- Business line / product approach versus portfolio approach
- Product capability compliance versus overall regulatory compliance
- Business maturity and business cycle
- Benchmarking and cross-industry collaboration
- Resource impacts, e.g. the work is never done
- End-to-end project and program commitment
- New certification / accreditation requirements, e.g. ISOs, SOC/SOC II, NIST, etc.

45

Pitfalls and Lessons Learned

Product and service development is more technical and global than ever before:

- Consider the use of offshore resources
- Contractual and regulatory barriers
- Training and certification requirements
- Communication and cultural issues
 - Example - Offshore team won't tell leadership they are off the rails
 - Example - That's a Brave Proposal!
 - Example - That's an interesting idea!
 - Example - Very interesting!

46

Pitfalls and Lessons Learned (cont.)

- Why is he doing my job?
 - Compliance Officer, Privacy Officer, Data Governance Officer, General Counsel, Clinical Officer, Safety Officer
 - CCO, JD, CCEP, CHC, CISO, CIO, SIRO
 - Who owns the issue, solution, knowledge to solve a barrier
 - The value of matrixed reporting, culture training
- Why do I have to fill out another form?
 - Establish required artifacts at beginning of development project
 - Evidence of compliance with requirements
 - Artifacts should be living documents

47

Pitfalls and Lessons Learned (cont.)

- Teams change
 - Don't assume everyone understands your role
 - Don't assume everyone knows the difference between compliance, privacy, legal, security, contracting, etc.
- Consider project cultural level setting at start
- Office hours aren't just for academia
- Out of site, out of mind – especially with remote teams and remote working – MAKE YOUR PRESENCE KNOWN

48

Small Group Fact Pattern

- You are the Compliance resource for a tooth brush manufacturer in White Plains, NY with manufacturing centers in Fort Worth, TX
- The company wants to enter the “smart tooth brush” space, where brush frequency, pressure, application, tartar level, etc. are monitored via bluetooth connection to a smart phone
- Inspired by his teenage daughter’s near constant social media activity, your CEO wants to give consumers the ability to upload their data onto an app where brushers can compare their brushing metrics against friends and family
- Your CFO does not want to budget for a privacy compliance professional, because “we already have a compliance officer” and she trusts you will “figure it out”
- Your CIO wants to develop the product in India, where she also would like to store data
- Sales wants to market the smart brushes online internationally because “our new customers can be anywhere in the world!”
- Your CEO just hired an “Agile Practitioner” to assist with the development and launch of the smart brush. They invite you to a daily scrum (which you find useless and challenging to attend given your new dual compliance and privacy role)
- You miss the quiet days when all you made was “normal” tooth brushes

49

Small Group Discussion

Directions:

Review the fact pattern and identify:

- The governance issues facing the team
- What governance role would typically be on point to solve that issue
- What solutions would help this team bring the product compliantly to market

50

Q & A

51



THANK YOU.

*Designing a Compliance and Governance Model for
Today's Hi-Tech Business Environment*

Annual Compliance & Ethics Institute | Gaylord National | National Harbor, MD
September 18, 2019
10:15 – 11:45am

52