



# Agile Innovation for Compliance

Minneapolis Regional Compliance & Ethics Conference

*March 6, 2020*

*1:00 – 2:00pm*

1



**Sarah Boswell-Healey**

Director

Privacy Compliance

Optum



**Eric Brotten, @ebrotten**

Director

Compliance

Optum



**Kyle Erickson**

Director

Product Security & Privacy

Medtronic

2

## Today's Presentation

- Evolution of Technology and Compliance Implications
- Agile and Compliance Support
- Lessons Learned
- Q&A

3

## Audience Survey Question

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

Do you work for a tech company?

A. Yes

B. No

5

## Evolution of Technology

### Example: Mobile Phone

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



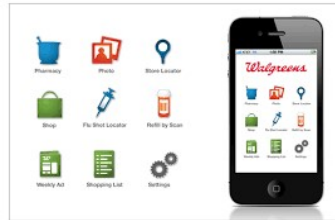
2019 – multifunctional tool: could be used as a phone, computer, a thermostat for your home, medical device?

6

## 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

7

## Evolution of Technology

“Every company is now a technology company”

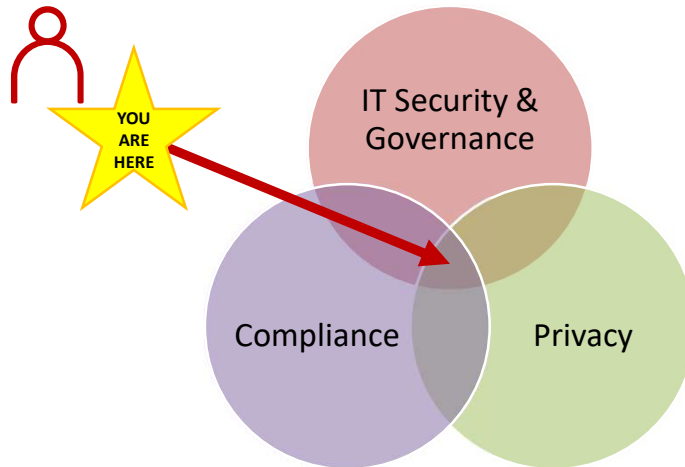
Journal, Dec. 4, 2018)

(Christopher Mims, The Wall Street



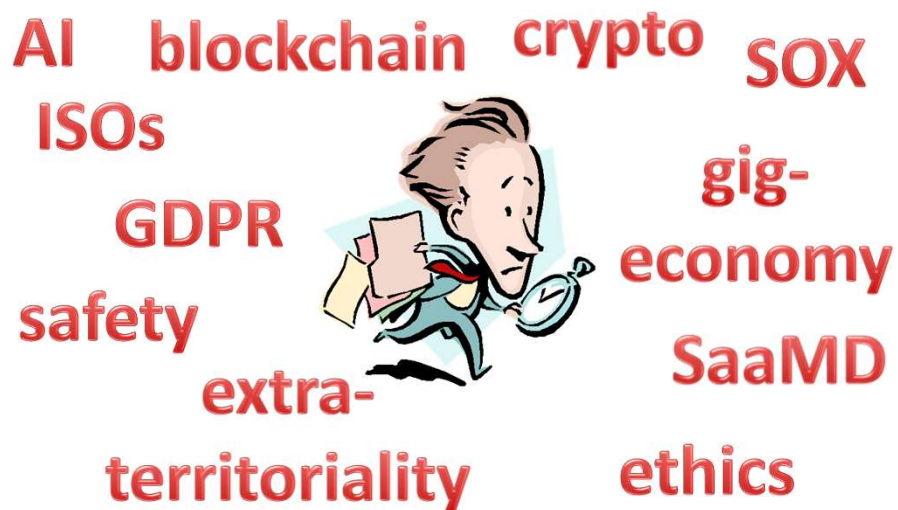
8

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



9

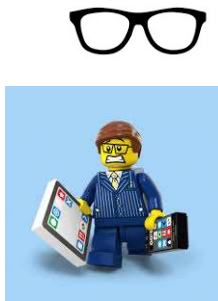
## Evolution of Technology: What Does It Mean For Today's Regulators?



10

## Today's Compliance Favors Diverse Work Experiences

**Eric:**  
Business/IT Product



**Sarah:**  
Museum/Waitress



**Kyle:**  
Help Desk / Web Dev



11

## Today's Compliance Favors Cross-Functional Teamwork



12

## Audience Survey Question

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?

13

## Product / Project / Service Delivery Development Methodology

### ***Traditional Waterfall***



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

14

## 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)

15

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

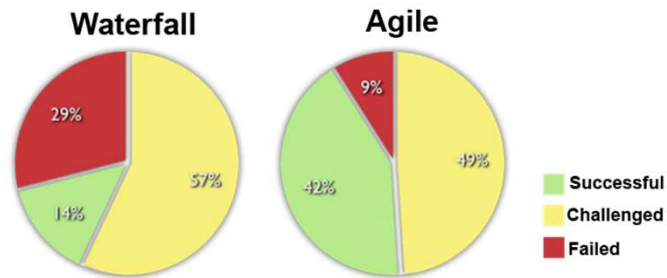
- No re-do's
- Bugs / errors
- Inflexible
- Speed to market slow (only when project done)



16



## The Solution: Agile

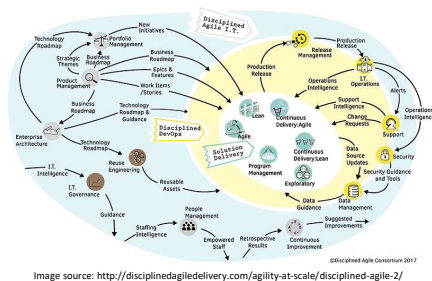


Source: the CHAOS Manifesto, The Standish Group, 2012

17

## Product / Project / Service Delivery Development Methodology

### Agile

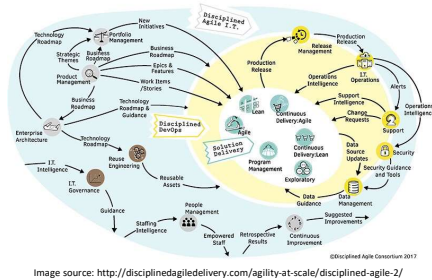


- Incremental
- On-going, small work packages
- On-going evaluation
- On-going design
- On-going releases

18

## Advantages for Your Business Partners

### Agile

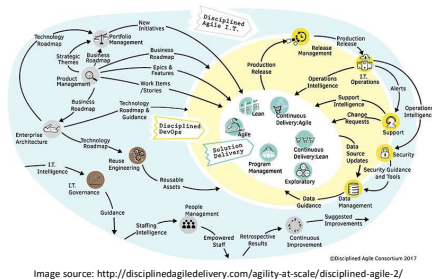


- Re-do's are allowed and expected
- Continuous feedback loops (and customer feedback)
- Less bugs / errors
- Speed to market fast as you want

19

## Challenges for the Compliance Practitioner

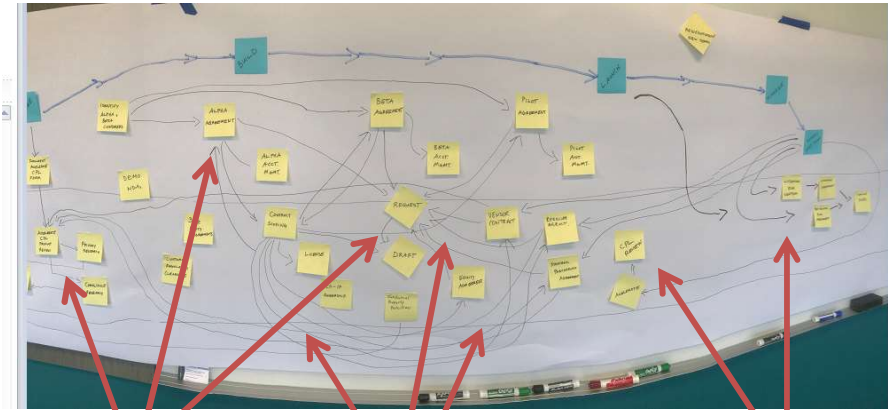
### Agile



- Fast paced project teams
- Multi-disciplinary stakeholder approach
- Lots of team meetings
- Need for continuous support

20

## Think You Don't Need to Learn Agile?



## EXTRA STEPS

## REWORK

WASTE

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

21

## Audience Survey Question

## 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>

22

## 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”



23

## The Transformation to Agile Compliance and Governance

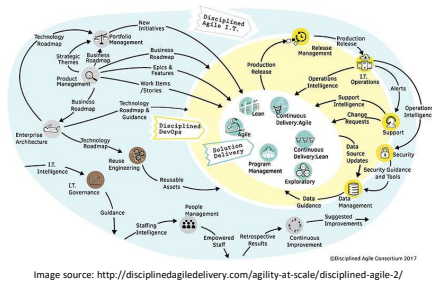


- Accept that your business partners will change their minds and course constantly
- Be solution-focused, not “Dr. No”
- Acknowledge the blurring lines across compliance, privacy, security, IT, and legal practitioners
  - Cross-train on areas of subject matter expertise
  - Avoid burnout and use shared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

24

# Implementing an “Agile” Compliance and Governance Support Model

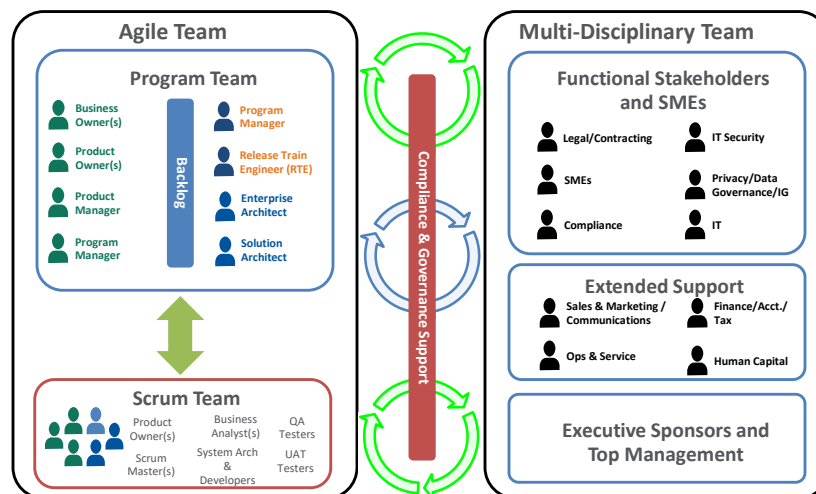
## Remember this? Agile



- 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!!!”

25

## What an Agile Compliance and Governance Team Looks Like



26

## How an Agile Compliance and Governance Team Operates

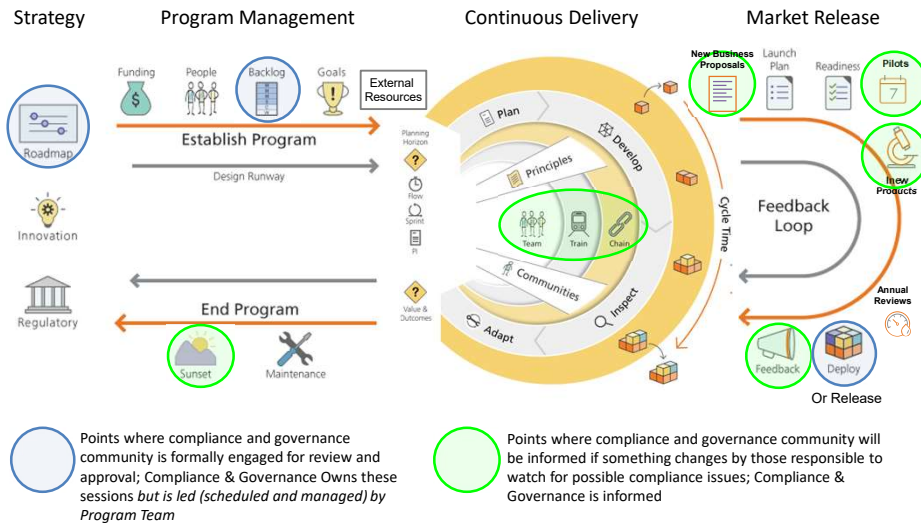


## Bonus Round 1

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



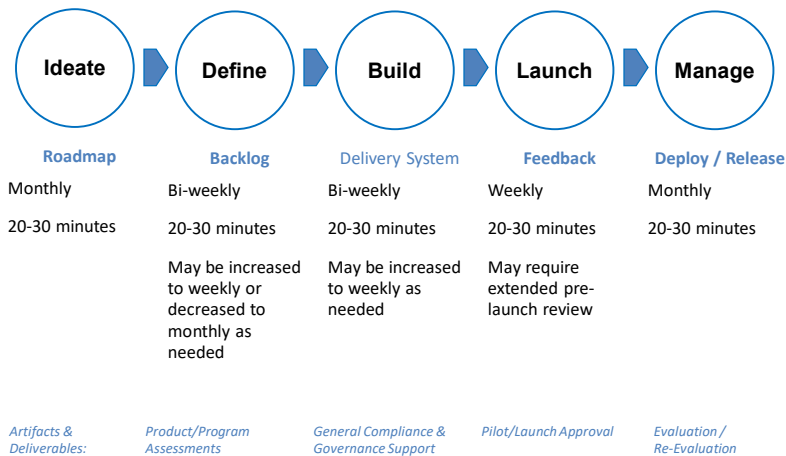
# Embedding Compliance and Governance into the Agile Delivery System



29

# Compliance and Governance Cadence within the Agile Delivery System

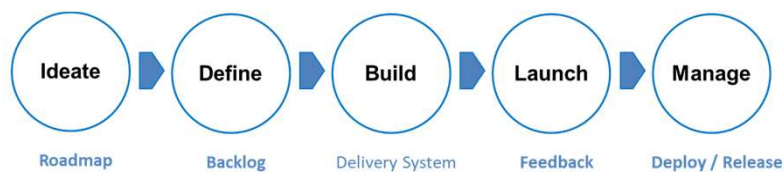
Team meeting pace recommended for products/programs according to the following development cycle phase:



30

## Bonus Round 2

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



31

## Artifacts & Tools for Success

- Roles & Responsibility Matrices (RACIs)
- Hazard Logs
- 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

32



## Bonus Round 3

[illegible]

## Other Tips and Considerations

## 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!

35

## 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

36

## 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**

37

## Q & A

38



THANK YOU.

*Agile Innovation for Compliance*

Minneapolis Regional Compliance & Ethics Conference

*March 6, 2020*

*1:00 – 2:00pm*

39

Appendix and Additional Resources

40

## 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.

41

## 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.






42

## 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.

43

## Agile Phase Descriptions

 <b>Roadmap</b>	 <b>Backlog</b>	 <b>Delivery System</b>	 <b>Feedback</b>	 <b>Deploy / Release &amp; Sunset</b>
<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"> <li>• Road mapping Sessions</li> </ul>	<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"> <li>• Project Management Council (PMC)</li> <li>• Feature Refinement</li> <li>• IGC Review</li> </ul>	<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&amp;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>

44

44

## IT Security Compliance Requirements Within Agile

Roadmap	Backlog	Delivery System	Feedback	Deploy / Release / Sunset
<ol style="list-style-type: none"> <li>1. Identify MVP IG/ ITSEC requirements for product based on emerging in-region market requirements</li> <li>2. Align business product roadmap with security architecture strategy identifying critical path items and gaps</li> <li>3. Utilize control portfolio to identify Secure DevOps Gaps</li> </ol>	<ol style="list-style-type: none"> <li>1. Delivery team to identify Capabilities that require security engineering of new patterns</li> <li>2. IG team sets clear definitions of done and acceptance criteria for key security capabilities (Eg: Authentication, SCA,)</li> </ol>	<ol style="list-style-type: none"> <li>1. Delivery team must establish scorecard of quality of delivery through SecDevOps processes</li> <li>2. Delivery team to utilize design patterns for security controls, or create new patterns</li> <li>3. Perform Security Architecture reviews</li> <li>4. Security &amp; Safety Champion will be established for each SCRUM team</li> </ol>	<ol style="list-style-type: none"> <li>1. Program Increments will demonstrate compliance and security functionality</li> <li>2. Secure DevOps will enforce DoD and AC defined for security, feedback given through scorecard review</li> </ol>	<ol style="list-style-type: none"> <li>1. Operational Readiness will ensure documented procedures for controls</li> <li>2. Delivery team will report on security testing and compliance</li> </ol>

45

45

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

46

## 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				

47

## Artifacts & Tools for Success: Hazard Logs

[illegible]

48



## Hazard Log Tips

- User stories should be sufficiently detailed to allow an informed hazard identification and assessment
- Initial hazard identification should be carried out in parallel to original user story capture. It is strongly recommended that a hazard workshop is run during the scoping phase to support complete hazard identification
- On-going hazard assessment processes should be included in sprint activities throughout the development life cycle, and are essential in providing further hazard identification and risk reduction
- Accurate cross referencing using unique identifier(s) should be used to maintain traceability between user stories and related identified hazards