"IT Governance and Compliance in an Agile World"

Presented by:

Bob Aiello
CM Best Practices Consulting

Brought to you by:

340 Corporate Way, Suite 300, Orange Park, FL 32073
888-268-8770 • 904-278-0524 • sqeinfo@sqe.com • www.sqe.com
Bob Aiello is a consultant, editor-in-chief of CM Crossroads, and author of *Configuration Management Best Practices: Practical Methods that Work in the Real World*, Bob Aiello is a consultant and software engineer specializing in software process improvement, including software configuration and release management. He has more than twenty-five years of experience as a technical manager at top New York City financial services firms, where he held company-wide responsibility for configuration management. He is vice chair of the IEEE 828 Standards Working Group on CM Planning and a member of the IEEE Software and Systems Engineering Standards Committee (S2ESC) Management Board. Contact Bob at Bob.Aiello@ieee.org, via LinkedIn, or visit cmbestpractices.com.
IT Governance and Compliance in an Agile World

Bob Aiello, Principal Consultant and Author of *Configuration Management Best Practices: Practical Methods that Work in the Real World*

http://www.linkedin.com/in/BobAiello
http://cmbestpractices.com

Who am I?

- CM Lead & Consultant for over 25 years
- Editor-in-Chief at CM Crossroads
- Author of CM Best Practices
- IEEE Management Board
- Tools and process agnostic
- The guy the auditors call on!
Books, Articles & Webcasts

- Mike Huetterman – Agile ALM
- Mario Moreira – Adapting Configuration Management for Agile Teams
- Agile Journal
- Developerworks
- CM Journal
- ALM Journal
- ITSM Portal

Published on Audit for Agile

Adapting Configuration Management for Agile Teams: Balancing Sustainability and Speed by Mario Moreira

CM that is adapted to suit the continuous nature of change that Agile provides without sacrificing the values of CM.
Agile Configuration Management

Individuals and interactions over processes and tools
Working software over comprehensive documentation
Customer collaboration over contract negotiation
Responding to change over following a plan

Agile World

• Focus on individuals and interactions
• Working software
• Customer collaboration
• Welcome change even late in the process
• Rapid iterative development
Agile Works!

• Avoid documenting requirements we do not (yet) understand
• Managing risk
• Decisions at last responsible moment
• Honesty regarding what we know

Test Cases at the NYSE

• POS Displaybook used by the Specialist
• Challenged the user rep to write test cases
• The first hour we determined that “what we have asked for is not what we want”
• Examining milestone releases while writing test cases is essential!
Agile Misconceptions

- Coding without requirements
- Lack of processes & tools
- Lack of documentation
- No contracts
- No plans

Goals of Agile CM

- Rapidly build, package and deploy
- Reliable and repeatable process
- Traceability and forensics
- Emergence of DevOps
Characteristics of Agile CM

- Customer-centric (which one?)
- Rapid iterative development
- Pragmatic approach to requirements
- Support for testing
- Collaborative communication
- Role in the SCRUM

Knight Capital

- August 1st outage
- Erroneously purchased 7 billion dollars of stock
- Loss of 440 Million dollars
- Old software that was left on the system
- Lack of DevOps
Batman and Superheros

• Lucious Fox warns Batman about a possible malfunction in autopilot for the “Bat”
• Batman’s own life depends upon the autopilot
• Patch was documented by Bruce Wayne

SEC Investigation

• Lack of controls
• Proper testing & process
• Impact to shareholders
• Impact to market
Banks

- Compliance with SOX
- Office of the Currency - Treasury
- FFIEC – Federal Financial Institutions Council

And government agencies…

---

GAO

- FDIC cited
- Numerous government agencies cited
- Lack of controls
- Failing internal audit
Agile Focus

• Productivity
• Quality
• Did we mention working software?
• Agile testing

Deming – Build Quality In

• Verification – meeting requirements
• Validations – are the requirements correct?
• Agility helps us build quality in from the beginning
• Test cases and scripts are valuable artifacts
IT Governance

- IT Governance needs to be in alignment with corporate governance
- Provides transparency
- Helps senior management make the right decisions
- Educate your boss!

ISACA Board Briefing on ITG

Fundamentally, IT governance is concerned about two things:
- IT's delivery of value to the business
- Mitigation of IT risks

Source www.isaca.org
**Compliance**

- Usually to regulatory requirements
- Interpreted based upon frameworks such as Cobit
- Financial reports need to be accurate

**Examples**

- Separation of controls
- Steps are logged - including results
- Traceable to the Change Request
- Security measures to prevent unauthorized changes
- Audit in place for intrusion detection
What Are the Regs?

- Section 404 of the Sarbanes-Oxley Act of 2002
- HIPPA and CFR 21
- SSAE 16 (formerly SAS 70)
- Audit requirements

What is Agile Process Maturity?

- Adherence to the principles (purity)
- Scalability (Scrum of Scrums)
- Transparency and traceability
- Coexistence with Non-Agile
- Consider the items on the right
Agile Process Maturity

- Repeatable process
- Tools matter
- Adequate documentation
- Contracts required
- Gotta have a plan

Emergence of DevOps

- Agile Systems Administration
- Critical with rapid iterative development
- Development is not taking over Ops
- Synergy of development and Ops
Moving Upstream

- Developing automated build, package and deployment early in the process
- Starting in development
- Developing the automation is a project itself
- Using Agile principles

Virtual Build Engineer

- Separate Build Engineer Account
- Completely automated
- Provides traceability
- Logging and reporting
Agile Views

What are some of the views of others in the Agile Community?

Agile Release Train (ART)

Making each product a successful and routine event – an event that is indeed planned and eagerly anticipated, yet one that happens almost on autopilot

Dean Leffingwell’s Agile Software Requirements, p. 299
Deployment Pipeline

A deployment pipeline is … an automated implementation of your application’s build, deploy, test and release process

Jez Humble and David Farley’s Continuous Delivery, p 3.

Aim of the Pipeline

• Makes building, deploying, testing and releasing software visible to everyone involved
• Improves feedback so that problems are identified, and so resolved, as early in the process as possible
• Enables teams to deploy and release any version of their software to any environment at will through a fully automated process (p. 4)
Antipatterns

- Deploying Software Manually
- Deploying to Production-like environment only after Development is complete
- Manual Configuration of Production Environments

Continuous Deployment, p. 7 – 10

Devops

- Synergy of Agile & ITIL
- Full lifecycle approach
- Good communication to all stakeholders
- Break down barriers
- Don’t forget separation of roles
Dev/QA Focus

• Development
• QA & Testing
• Operations
• Self-Managing/Organizing Teams

Sox Compliance

• Section 404 of the Sarbanes-Oxley Act of 2002
• Using ISACA Cobit 4.1
• 34 high level IT controls
• PCI compliance
• SSAE 16 (formerly SAS-70)
ISO 9001

- Establishes the quality management system (QMS)
- ISO 90003 is the software standard in the 9000 family of standards
- Uses ISO 12207 (or 15288) to specify lifecycle processes
- ISO 10007 for CM
- IEEE 828, EIA 649-B, Mil Std coming!

Which Standards?

- IEEE 828 – CM Planning
- EIA 649-A – Non-compliance
- ISO 90003 to support QMS
- Full lifecycle ISO 12207

Tailor!
Moving Upstream

- Dev to CM to QA to Ops
- Cross-functional focus
- Speed up development
- Build a great deployment architecture
- Give it to Devs as a service!

Frameworks

- ITIL v3 including CMDBs, federated CMDBs, CMS, DML…
- Cobit for SOX
- CMMI ->>> Agile
**Configuration Management**

- Configuration Identification
- Status Accounting
- Change Control
- Configuration Audit

*Tracking and Controlling Changes to Configuration Items*

---

**Your Agile Process**

- Should be Lean
- Processes need to be reviewed
- Tailor down or tailor up
- More collaboration and consensus building
- Use standards and frameworks
**Assessment**

- First step is to assess current practices - “As-Is”
- Compare to industry standards and frameworks
- Determine “To-Be”
- Create a plan for improving your CM processes

---

**Plan for Improvement**

- Improve training and use case for source code management
- Improve build automation
- Set up or improve continuous integration
- Automate package and deployment
- Create procedures for configuration audit
IT Governance and Compliance in an Agile World

Bob Aiello, Principal Consultant and Author of
Configuration Management Best Practices: Practical Methods that Work in the Real World

http://www.linkedin.com/in/BobAiello
http://cmbestpractices.com