Surviving SOX with Scrum

Integrating Scrum in IT Governance at Allianz
Simon Roberts, Christoph Mathis
http://scrumcenter.com
Christoph Weiß, Allianz Deutschland AG
Who are we?

Simon Roberts and Christoph Mathis
Independent Scrum coaches and trainers; Scrum since 2002, light-weight methods since late 1990s
Both have a strong software engineering background
Track record of successful Scrum projects for small, medium and large enterprises in Germany and the UK

Christoph Weiß
SOX coordinator @ Allianz
christoph.mathis@scrumcenter.com
simon.roberts@scrumcenter.com
christoph.weiss@allianz.de
What are we going to talk about?

- Scrum @ Allianz Germany
- Potential impediments
- The governance landscape
- What is SOX?
- Why might it be important for your company?
- Potential conflicts
- What requirements does SOX place on IT?
- How does Scrum help?
- Examples
- Summary
Scrum - Eine Reise

Es geht los!
Scrum @ Allianz
A Holistic Approach

- We have been engaged in a Scrum transition at Allianz Germany for the last 2 years
- For us, Scrum in the Enterprise includes at least:
  - How to transition to Scrum and sustain its use through change management
  - How to integrate with IT governance
  - How to help teams, Product Owners and Scrum Masters to realize their potential
- Today we want to talk mainly about integrating Scrum with IT governance but first let's take a look at our enterprise Scrum approach in a little more detail ...
**Sponsor**
- Hire outside help

**Initiate**
- Light the first beacon

**Ignite**
- Create a center of excellence

**Professionalize**
- Achieve executive buy-in

**Promote**
- Light further beacons

**Diversify**
- Light even more beacons

**Establish**
- Initiate an Enterprise Transition process

**Consolidate**
- COBIT, CMMI, SOX

**Integrate**
Scrum in the Enterprise

Some typical and some not-so-typical impediments
Der Tyrann
der Wasserfälle
Das Command-und-Control-Monster

Nein!

Teambildung / Organisation
Der Vogel Strauß der Prozesse

Ne-ne, das klappt schon!
Geh weg mit dem Neuen!
Der Methoden-Zauberer

schnell
einfach
problemlos
reibungs- und
treibfri
mühelos
The Enterprise Scrum Governance Landscape
What is SOX?

- Sarbanes-Oxley Act
- Technically a U.S. law from 2002 which is intended to ensure the reliability of financial statements of public companies
  - in the wake of the scandals around Enron, WorldCom and others
  - New: the leaders of an organization are personally responsible for compliance and for the correctness of financial statements
- SOX 404 (the part most important for IT):
  - Public companies must introduce strict internal controls
  - They must document these controls
  - guarantee that they are followed
  - test their design
  - test their effectiveness
The History of Compliance in the USA

- 1933: SEC (Securities and Exchange Commission) and GAAP (Generally Accepted Accounting Principles)
  - introduced after the depression of 1929
- 1985: Treadway Commission
  - after a series of financial scandals, the Treadway Commission (named after James Treadway, former chairman of the SEC) brought together leading accounting organizations:
    - FEI (Financial Executives International)
    - AAA (American Accounting Association)
    - AIPCA (American Institute of Certified Public Accountants)
    - IIA (Institute of Internal Auditors)
    - IMA (Institute of Management Accountants)
  - this became known as COSO (Committee of Sponsoring Organizations of the Treadway Commission)
Why might SOX be relevant for your Organization?

- If you have a US listing
- If you need access to the capital markets
- SOX is becoming a de facto standard outside the US
- Analysts increasingly include IT governance in their rating of an organization, which can have an effect on stock price
- The EU Commission is going in a similar direction with their focus on the COBIT framework
- The financial crisis will likely result in stricter controls
Cost of SOX

In the USA companies spend 6 billion US $ annually on SOX compliance activities
Potential conflicts with SOX
comply and die: static business model

Profitable, Agile Enterprise

Potential conflicts with SOX
comply and die: static business model
non-compliance penalties

Potential conflicts with SOX
comply and die: static business model

inefficient processes

non-compliance penalties

Product with SOX
comply and die: static business model
non-compliance penalties

inefficient processes high compliance costs
What Requirements does SOX place on IT?

- Important SOX relevant controls of the CobIT Framework include
- Defined Development Process
- Defined Deployment Process
- Prevention of Manipulation (Segregation of Duties)
- Performance Management
- User Documentation
- Testing
- Versioning and Archiving
<table>
<thead>
<tr>
<th>Goal</th>
<th>Realization</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined development process</td>
<td>Scrum is a defined framework which can form the basis of a defined process</td>
<td>Need to standardize practices</td>
</tr>
<tr>
<td>Defined deployment process</td>
<td>Integrate release decision making into Sprint review</td>
<td>Dual-key deployment</td>
</tr>
<tr>
<td>Prevention of manipulation</td>
<td>Additional user stories for some applications</td>
<td>Access rights for key data and acceptance-tested final code</td>
</tr>
<tr>
<td>Performance management</td>
<td>Resource allocation at the technical level</td>
<td>Need to guarantee that financial information is produced in a timely manner</td>
</tr>
</tbody>
</table>
## SOX Requirements and Scrum

<table>
<thead>
<tr>
<th>Goal</th>
<th>Realization</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testing</td>
<td>Automated testing, test definitions and reports securely archived</td>
<td>Possible to leverage continuous build and test system</td>
</tr>
<tr>
<td>Documentation for Users</td>
<td>Additional acceptance criteria for user stories or additional user stories</td>
<td>The documentation that SOX requires becomes part of the definition of done</td>
</tr>
<tr>
<td>Versioning and Archiving</td>
<td>Has an impact on the configuration management systems that we use and introduces additional requirements on applications that we can represent as user stories</td>
<td>Need to archive productive program versions and balance relevant data for at least 10 years</td>
</tr>
</tbody>
</table>
Defined Development Process

- Sprint
- Daily Scrum
- Sprint Review/Retrospective
- Release Planning
- Sprint Backlog
- Sprint Planning
- Product Backlog
- Product Increment
- Sprint
- Burn Down Chart
- Daily Scrum
Defined Development Process

Standardized Practices:
• Project Charter
• User Stories
• Story Points
• Planning Poker
• Automated Unit Testing
• Automated Acceptance Testing
• Continuous Integration
User Stories for SOX

Relevant Projects (1)

Auto Insurance Discount

As an insurance agent

I want to be able to offer a potential customer a discount

so that I have a better chance to be competitive and win her business
User Stories for SOX

Relevant Projects (1)

**Auto Insurance Discount**

As an insurance agent

I want to be able to offer a potential customer a discount

so that I have a better chance to be competitive and win her business

**Acceptance Criteria**

- Discount input as percent from a fixed set of options in a drop down list
- Check discount is displayed correctly in policy summary and that premium reflects discount
- Check discount value transmitted to mainframe correctly
- Check mainframe receives correct value
- Check DB timestamp and "who altered" flags set correctly
User Stories for SOX

Relevant Projects (2)

List of Discounts Awaiting Approval

As a discount approver

I want to see a list of discounts waiting for approval

so that I can get the information that I need to control my discount budget
User Stories for SOX
Relevant Projects (2)

List of Discounts Awaiting Approval

As a discount approver

I want to see a list of discounts waiting for approval

so that I can get the information that I need to control my discount budget

Acceptance Criteria

- Monetary impact of discount visible?
- List of open discount cases visible?
Accept, Reject or Change Discount

As a discount approver

I want to accept, refuse or change a discount case

so that I can control my budget
User Stories for SOX
Relevant Projects (3)

Accept, Reject or Change Discount

As a discount approver

I want to accept, refuse or change a discount case

so that I can control my budget

Acceptance Criteria

- Accept a discount – check DB updated accordingly
- Refuse a discount – check DB updated accordingly
- Change the amount of a discount – check DB updated accordingly
- Check processed entries are removed from the list
- Check that same entry can't be processed by two different approvers at the same time
- Check printed contract reflects changes made
- Check mainframe gets new information correctly
**User Stories for SOX**

**Relevant Projects (4)**

---

**Feedback for Insurance Agent**

As an insurance agent

I want to get feedback on not yet approved and rejected discount cases

so that I can give feedback to my customers on the current state of their insurance application
Feedback for Insurance Agent

As an insurance agent

I want to get feedback on not yet approved and rejected discount cases

so that I can give feedback to my customers on the current state of their insurance application

Acceptance Criteria

- Check that rejected discounts are displayed as rejected in the list
- Check that not yet processed discounts are displayed in the list
- Check that only the discounts cases for this particular insurance agent are displayed
Only Approvers Can Approve

As the SOX Controller

I want to ensure that only users with the "approver" permission can approve a discount case

so that I can ensure that other users cannot manipulate balance relevant data
User Stories for SOX

Relevant Projects (5)

Only Approvers Can Approve

As the SOX Controller

I want to ensure that only users with the “approver” permission can approve a discount case

so that I can ensure that other users cannot manipulate balance relevant data

Acceptance Criteria

• Check that a user without this permission cannot approve discounts
• Check that a user with this permission can approve discounts
• Check that the system logs attempts to approve without having this permission (in DB)
<table>
<thead>
<tr>
<th>Test Case</th>
<th>Test Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>testNissan</td>
<td>Failed</td>
</tr>
<tr>
<td>testPeugeot</td>
<td>Passed</td>
</tr>
<tr>
<td>testFiatLkw</td>
<td>Passed</td>
</tr>
<tr>
<td>testOpel</td>
<td>Passed</td>
</tr>
<tr>
<td>testPortal404</td>
<td>Passed</td>
</tr>
<tr>
<td>testErstberater</td>
<td>Failed</td>
</tr>
</tbody>
</table>

```
junit.framework.ComparisonFailure: expected:<...64...> but was:<...52...>
at junit.framework.Assert.assertEquals(Assert.java:81)
at junit.framework.Assert.assertEquals(Assert.java:87)
at de.allianz.automotive.selenium.tarifrechner.NissanTest.performTestKomplettkennzeichen
at de.allianz.automotive.selenium.tarifrechner.NissanTest.testNissan(NissanTest.java:39)
```

```
com.thoughtworks.selenium.SeleniumException: ERROR: There was an unexpected
at com.thoughtworks.selenium.HttpCommandProcessor.doCommand(HttpCommandProcessor.java:73)
at com.thoughtworks.selenium.DefaultSelenium.windowFocus(DefaultSelenium.java:442)
at de.allianz.automotive.selenium.AbstractSeleniumTest.captureScreeshot(AbstractSeleniumTest.java:235)
```

Continuous Integration with Automated Acceptance Testing

Continuum, Maven and Selenium
Summary

- You might need to be SOX compliant even if your company does not have a US listing
- SOX and Scrum can coexist
- Some of the agile practices such as automated testing and user stories can help to make SOX compliance less painful
- For larger organizations, strict IT governance is unavoidable. Agile methods can help
... just one more thing
The key challenge is Compliance whilst Activating Innovation