Surviving SOX with Scrum

Integrating Scrum in IT Governance at Allianz
Who are we?

Simon Roberts MBA  and Dr. Christoph Mathis
Independent Scrum coaches and trainers; Scrum since 2002, XP 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
Together we provide the thought leadership for the Allianz Germany Agile Methods Competence Center
http://scrumcenter.org
Enterprise Scrum @ Allianz
A Holistic Approach

- We have been engaged in an enterprise Scrum transition at Allianz Germany for the last 2 years
- For us, enterprise Scrum 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

Initiate
Hire outside help

Ignite
Light the first beacon

Professionalize
Create a center of excellence

Diversify
Light further beacons

Promote
Achieve executive buy-in

Integrate
COBIT, CMMI, SOX

Establish
Light even more beacons

Consolidate
Initiate an Enterprise Transition process
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 the financial statement
- SOX 404 (the part most important for IT):
  - Public companies must introduce strict internal controls
  - They must document these controls
  - and guarantee that they are followed
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 for SOX-compliance activities.
Potential conflicts with SOX
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

Profitable, agile Enterprise
Potential conflicts with SOX

- profitable, agile enterprise
- non-compliance penalties

Comply and die: static business model
- inefficient processes
Potential conflicts with SOX
Profitable, agile Enterprise
comply and die: static business model
inefficient processes
non-compliance penalties
high compliance costs
<table>
<thead>
<tr>
<th>Goal</th>
<th>Realization</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined development process</td>
<td>Scrum as a defined process</td>
<td>Need to standardize practices</td>
</tr>
<tr>
<td>Defined release process</td>
<td>Integrate release decision making into Sprint review</td>
<td>Dual-key deployment</td>
</tr>
<tr>
<td>Prevention of manipulation</td>
<td>Access rights for key data and additional user stories for some applications</td>
<td></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>
<tr>
<td>Goal</td>
<td>Realization</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<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>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 balance relevant data for at least 10 years</td>
</tr>
</tbody>
</table>
Defined Development Process

1. Release Planning
2. Sprint Planning
3. Daily Scrum
4. Burn Down Chart
5. Sprint
6. Sprint Review/Retrospective
7. Product Increment

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

Standardized Practices:
- User Stories
- Story Points
- Planning Poker
- Automated Unit Testing
- Automated Acceptance Testing
- Continuous Integration

Product Backlog

Release Planning

Sprint Backlog

Sprint Planning

Sprint

Daily Scrum

Burn Down Chart

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint

Burn Down
Chart

Daily Scrum

Sprint Review/
Retrospective

Product Increment

Sprint

Backlog

Release
Planning

Sprint Planning

Sprint
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?
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
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
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
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)
Continuous Integration with Automated Acceptance Testing

Continuum, Maven and Selenium
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