Ensuring Governance in an Agile World

Sean Scranton, CISA, CISM, CRISC
Thad King, PMP

Agenda

• Background of RLI Insurance Company
• What is Agile?
• Where We Were
  • Governance, Security, and Compliance Issues
• Where Did We Need to Be
  • Identified improvement areas in the agile process to help ensure IT development is aligned with business requirements
• How Did We Get There
  • Mitigating Governance, Security, and Compliance Issues
  • Embedding security and controls requirements into the development process
  • Identifying appropriate methods of creating test cases and efficiently performing testing
  • Providing a feedback mechanism for the agile process for continuous improvement
Background of RLI

RLI Insurance Company (RLI)

- [http://www.rlicorp.com](http://www.rlicorp.com) (NYSE:RLI)
- Located in Peoria, IL, licensed in all 50 States.
- Specialty Insurance Company serving niche markets for over 45 years.
- RLI = Replacement Lens, Inc. Flagship Product in 1960 was contact lens insurance sold via optometrists.
- $850M(ish) top line, 2.7B in assets, A+ A.M. Best Rating.
- Entrepreneurial culture and continued appetite for organic and inorganic growth.
RLI Insurance Company (RLI)

Underwriting Profit

RLI has achieved 16 straight years of a combined ratio below 100, and has beaten the industry ratio by an average of 15 points.

STATUTORY COMBINED RATIO

<table>
<thead>
<tr>
<th>Year</th>
<th>RLI</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>'01</td>
<td>96</td>
<td>100</td>
</tr>
<tr>
<td>'02</td>
<td>92</td>
<td>100</td>
</tr>
<tr>
<td>'03</td>
<td>93</td>
<td>100</td>
</tr>
<tr>
<td>'04</td>
<td>94</td>
<td>100</td>
</tr>
<tr>
<td>'05</td>
<td>87</td>
<td>100</td>
</tr>
<tr>
<td>'06</td>
<td>84</td>
<td>100</td>
</tr>
<tr>
<td>'07</td>
<td>73</td>
<td>100</td>
</tr>
<tr>
<td>'08</td>
<td>86</td>
<td>100</td>
</tr>
<tr>
<td>'09</td>
<td>84</td>
<td>100</td>
</tr>
<tr>
<td>'10</td>
<td>81</td>
<td>100</td>
</tr>
<tr>
<td>'11</td>
<td>79</td>
<td>100</td>
</tr>
<tr>
<td>'12</td>
<td>88</td>
<td>100</td>
</tr>
<tr>
<td>'13</td>
<td>82</td>
<td>100</td>
</tr>
<tr>
<td>'14</td>
<td>84</td>
<td>100</td>
</tr>
<tr>
<td>'15</td>
<td>84</td>
<td>100</td>
</tr>
</tbody>
</table>

RLI Insurance Company (RLI)

- Distributed Insurance Operations, Centralized Home Office Support functions.
- 800+ Employees, 50+ Locations.
- IT Department in Peoria, IL with some remote Developers.
- Structured into various Solutions teams, Shared Services Team, and Technology/Architecture team.
- Strong Microsoft Shop for Development.
- Best of Class for non-core functions.
- The usual challenges – balancing legacy, e-legacy and new technology.

IT Spending as a % of GWP

- Industry: 3.5%
- RLI: 2.3%
What is Agile?

Agile

- A framework for development based on empowered teams to respond to unpredictability through iterative cadences
- Variations include Safe, Scrum, XP, Lean, Kanban, and many more
How Is Agile Different from Waterfall?

<table>
<thead>
<tr>
<th>Waterfall</th>
<th>Agile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upfront Design</td>
<td>Design Integrated</td>
</tr>
<tr>
<td>Contracts</td>
<td>Collaboration</td>
</tr>
<tr>
<td>Cold handoffs</td>
<td>Face to Face Communication</td>
</tr>
<tr>
<td>Lessons Learned – Postmortem</td>
<td>Frequent Retrospectives</td>
</tr>
<tr>
<td>Work shifts teams concurrently</td>
<td>Manage Flow</td>
</tr>
<tr>
<td></td>
<td>Limit Work in Process</td>
</tr>
</tbody>
</table>

Agile Manifesto

We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

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

That is, while there is value in the items on the right, we value the items on the left more.

Source: www.agilemanifesto.org
Ongoing Collaboration

Where We Were
We Had Some Issues – Portfolio-Level

• There is a lot going on, but nothing seems to be moving
• It is difficult to change decisions late in the process
• Long or complex projects are difficult to complete
• Tell us what you want now and we will get back to you in a year
• Testing is either very long or too high level, and is sacrificed in order to meet deadlines
• We were just audited and we need to rewrite the system to address the audit issues!

We Had Some Issues – Project-Level

• Example project – conversion of legacy system to “off the shelf” system
• Too little communication between departments
• Fear of disjointed operational processes by switching systems
• New requirements came as frequently as old requirements changed
• No minimum viable product was envisioned
• Lots of pieces in the air at the same time – too much multitasking
• “Audit Requirements” came later
We Had Some Issues – Controls

- System security was almost an afterthought
- Knew we had to interface with other systems, and at some point we would need to do reconciliations and exception reporting
- Testing was something we did during training
- At some point Audit would come around and look at systems controls
- Overall Result: Internal Audit tried to get involved with *every* large project
- Eventually, IT called in the cavalry

Where Did We Need to Be?
Where Did We Need to Be?

- Partnered with Third Party (the cavalry) to perform an overall assessment of ALM (Application Lifecycle Management)

ALM Assessment Findings

- Lack of built-in quality (code reviews, unit testing, automated testing) lead to maintenance issues
- Development processes and management were inconsistent between teams – process communication
- Fear of Innovation / Change
  - Learn from it, good or bad
  - Lots of small improvements add up quickly
- Assessment vendor provided recommendations and action plans, and a simple maturity model for use as a gap analysis
ALM Rec and Action Plans (Governance)

- Not Governance that is agile, rather, Governance that supports agile
- Not overhead – integral part of the methodology

Main Themes:
- Portfolio Management
- Scheduling / Cadences
- Requirements Definitions
- Testing
- Security / Controls
- System Interface Controls
- Access Controls
- Vulnerability Assessments
- Training
- Continuous Improvement

How Did We Get There?
Portfolio Management

- Needed to ensure IT efforts were Aligned with the Business
  - Governance became the shim between IT and the Business
    - Business = PMG (Project Management Group) / Product Owners
  - Portfolio Level – APO02 / APO05 Manage Strategy / Portfolio
  - Project Level – BAI01 Manage Programs and Projects
  - Scheduling / Cadence

- Communication among stakeholders / prioritization (along the horizontal)
  - Communication effective and timely; confirm IT-related objectives are in line with Business
  - Redefined our intake process to ensure cross-team discussions
  - Ongoing Scrum-of-Scrum, consistent Product Owner Involvement

Just In Time Sizing

- Roadmap planning
- Release planning

Increasing Precision
- T-shirt: L, M, S
- Swag: days/hours
- Task breakdown

Project Throttling
- Don’t estimate more than can fit
Scheduling / Cadence

- Needed to align Project Management / Portfolio cadence with IT cadence
  - Was not as hard as it sounds
  - Smallest level of an application the Business discusses is a “Feature”
  - Features may take one or several sprints
  - Features are broken down into more manageable tasks for IT

- Difficulty with scheduling work to the teams
  - Small organization, many developers worked on different projects
  - APO07 Manage Human Resources (APO07.05)
  - Time tracking invaluable – we can predict available resources

Scheduling – Resource Planning (Portfolio)
Scheduling – Resource Planning (Team)

• Team-Level Planning

• Resource-Level Planning

Requirements Definition

• Previous Waterfall projects would have detailed requirements, but the Business Use case had often changed by the time of implementation

• Requirements are now created as close to the development as feasible

• Product Owner drives requirements and defines the true needs

• Test Cases are now developed from requirements!

• BAI02 Manage Requirements Definition
Testing

- Testing occurs throughout Development, not just at the end
- As Batch Sizes (sprint times) are reduced, there is an increased need for Testing Automation
  - Limits us to our current maturity level
- Key is to write requirements that can be directly converted into an Acceptance Test
- APO11 Manage Quality
- BAI07 Manage Change Acceptance and Transitioning
Security / Controls

- Previous Waterfall developments would add security needs and controls near the end of the project
- These are now integrated into the overall project
- Examples
  - System Interfaces – Exception Reporting / Reconciliation Reports (DSS06 Manage Business Process Controls)
  - Access Controls – Configuration and Access Reports (DSS06 Manage Business Process Controls)
  - Vulnerability Assessments (DSS05 Manage Security Services)

Security / Controls

- Note that System Interface and Access Control needs are part of Development sprints
- Vulnerability Assessments are performed once the system reaches Q/A
  - Performed out-of-band from sprint cadence
  - Feedback provided to Developers
Training

- Previously, training was ad-hoc, and occurred during Testing
- Training begins once system enters Q/A
- Still have some room to go with Training
- BAI08 Manage Knowledge

Continuous Improvement

- Continuous Improvement reviews baked in across the spectrum
  - APO11 Manage Quality (Portfolio / Project)
  - BAI07 Manage Change Acceptance and Transitioning (Project)
    - BAI07.08 – Post-Implementation Review
  - MEA01 Monitor, Evaluate and Assess Performance and Conformance
- Teams have retrospectives to adjust what is not working, enhance what is
  - Governance does the same
Resources

- SAFe (Scaled Agile) Framework - [www.scaledagileframework.com](http://www.scaledagileframework.com)
- The Principles of Product Development Flow; Donald G. Reinertsen
- Succeeding with Agile Governance – The Agile PMO; Paul Osborn
- The Phoenix Project; Kim / Behr / Spafford
- COBIT 5

Questions?

- Thank You!
- Sean Scranton, sean.scranton@rlicorp.com
- Thad King, thad.king@rlicorp.com