Enabling Regulatory Compliance for Software Engineering

Aaron Massey, Sreedevi Sampath, and **Carolyn Seaman**

UMBC, Baltimore, MD

Narration at: https://www.youtube.com/watch?v=k9wLQEvh2Hw

Core research question

How can software engineers incorporate and demonstrate regulatory compliance throughout the design, development, and maintenance of software systems?

Increasingly, organizations that develop software are required to ensure it complies with laws and regulations. Demonstrating regulatory compliance requires new mechanisms, processes, and tools throughout the software development lifecycle. Our goal is to develop a complete methodology, based on current practice and research, to help software engineers, policy makers, and regulators build and assess software systems

Challenges to demonstrating regulatory compliance throughout the SDLC include:

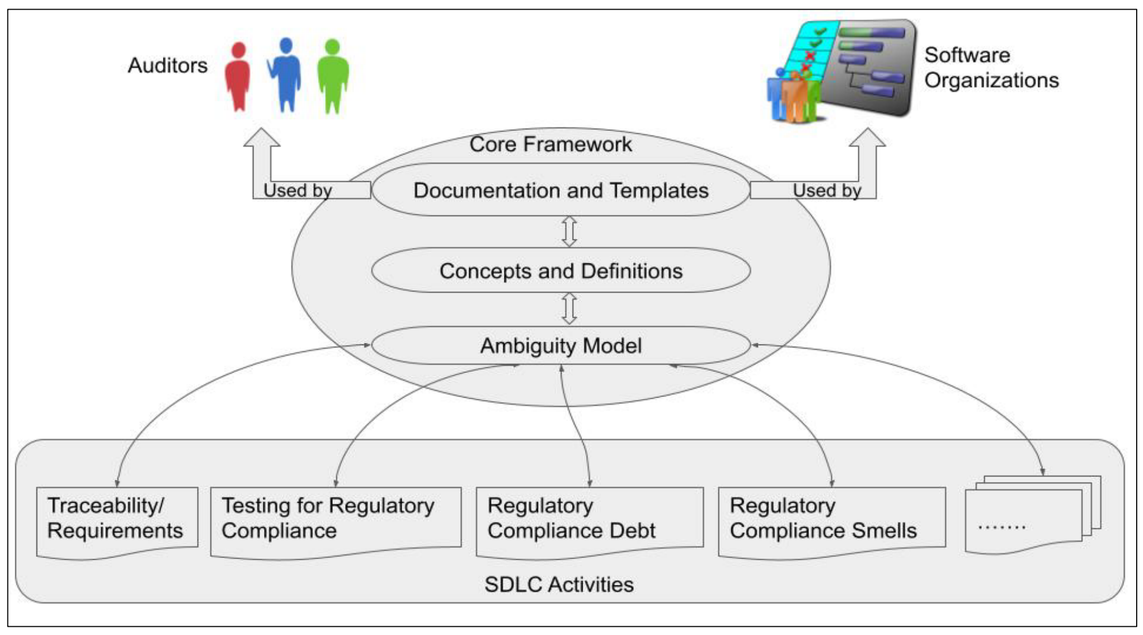
- management of both intentional and unintentional regulatory ambiguity;
- communication between stakeholders from disparate domains, (e.g., lawyers, policy makers, regulatory agencies, developers, managers, and testers);
- a dearth of methods for testing and maintaining regulatory compliance of software

If we're successful:

- We will provide a software development methodology, with supporting techniques, for regulatory compliance.
- Software providers will be able to both
  - manage regulatory compliance during software development and
  - demonstrate to outside auditors, customers, and the public, their approach towards compliance at each stage of the SDLC.

Key elements of solution:

1. Grounded definitions, concepts, models, and templates for regulatory compliance
   - Interview study of a variety of stakeholders
   - Case study observing developers reasoning about legal ambiguity
2. Focus on gaps in techniques for software testing and maintenance
3. Iterative evaluation of our work from a community of practitioners



Broader impacts on society

This research potentially affects every software system used in a regulated domain (e.g., health care, finance, etc.) touching all aspects of society. Its effects could extend to all activities in those domains; from preventative measures for a compliance failure to post hoc analysis and auditing of realized non-compliance.

Broader impacts on education

- The training of future researchers
- Results will be published in peer-reviewed conferences and journals
- Results will be incorporated into course materials (e.g., security and privacy courses)

Broader participation impacts

- UMBC is an R1 Minority-serving institution
- Promoting inclusion of underrepresented minorities in computing research
- Transforming how software organizations think about liabilities

Add Your Logo and/or project info h
Award ID#: