Open Source Compliance: Art or Science?

Ibrahim Haddad, Ph.D.
Head of Open Source Innovation Group
Samsung Research America – Silicon Valley

@IbrahimAtLinux

Compliance 101

- Users of open source software must observe all the copyright notices and satisfy all the license obligations for the FOSS they use.

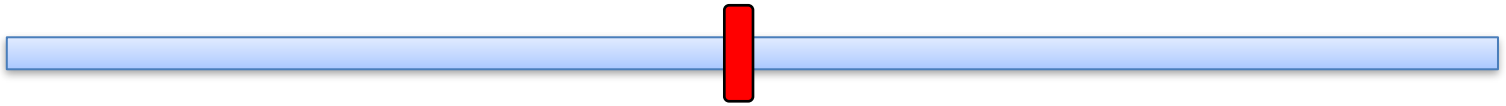
- Companies using open source software in commercial products, while complying with the terms of FOSS licenses, want to protect their intellectual property and that of third party suppliers from unintended disclosure. Hence, two additional conditions added to ensuring compliance from commercial users.

The Compliance Approach

- Policy
- Process
- Guidelines
- Staffing
- Training
- Audits
- Tools
- Automation
- Inquiries / Challenges

Art or Science
A Game of Percentages

Art / Science Compliance Meter



Art
(Creative Activity)

Science
(Systematic Approach)

Stories

- All stories are real.

- Company names and specifics are removed to protect the innocent ;-)

Policy

- **STORY #1: <u>The 1 line policy.</u>**

We must ensure that all of <COMPANY NAME>'s incoming software (in house, 3rd party commercial, open source, other) is compliant with the license it is provided under by following the open source compliance process defined in <URL>.

Policy

- **STORY #2: <u>The 72 pages master policy</u> (that probably very few read if any).**

  +

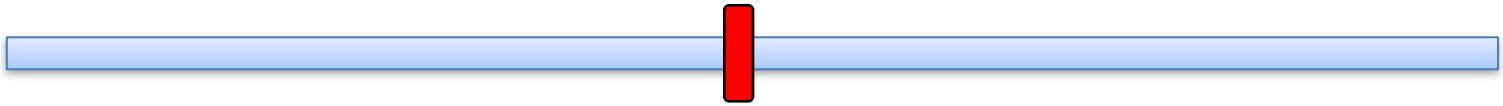
  Various mini policies ranging from 10 to 22 pages

[22 pages = Open Source Compliance Practices When Engaging With Business Partners]

<u>Fun Fact:</u>

1 policy page per 1000 employee. The math works!

Policy: Art / Science Meter

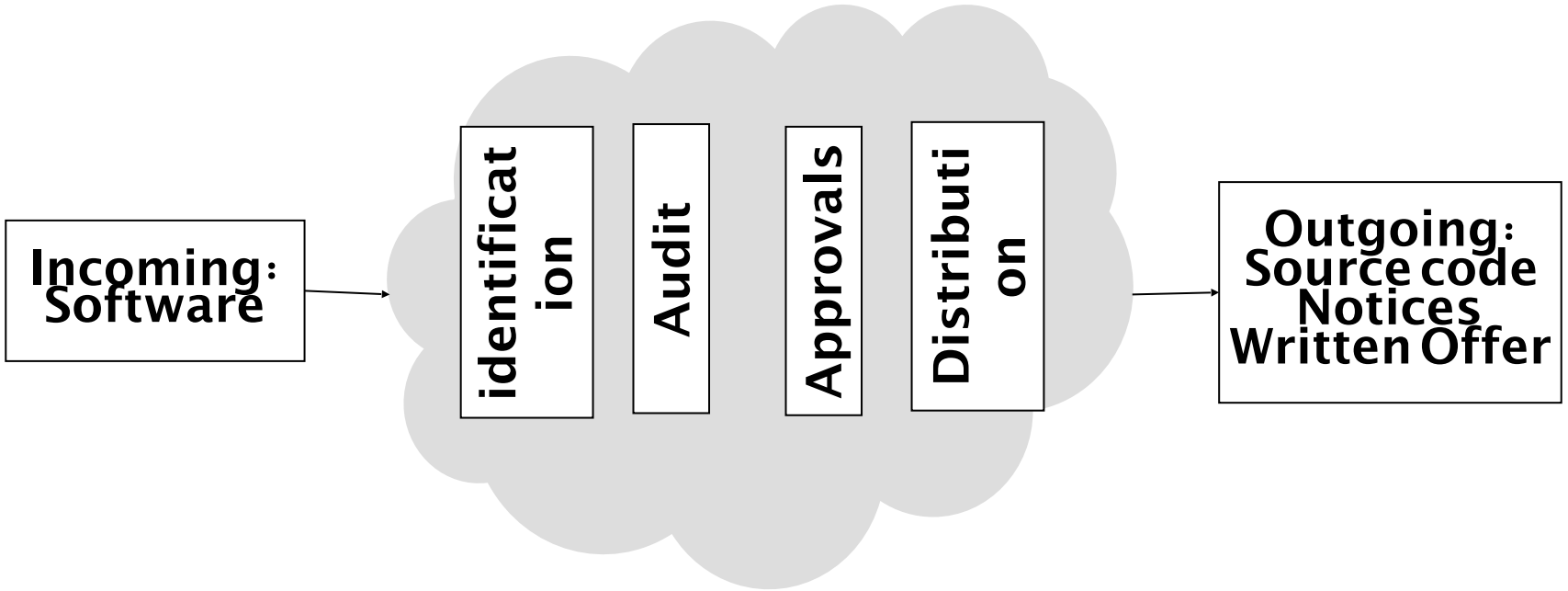


Art
(Creative Activity)

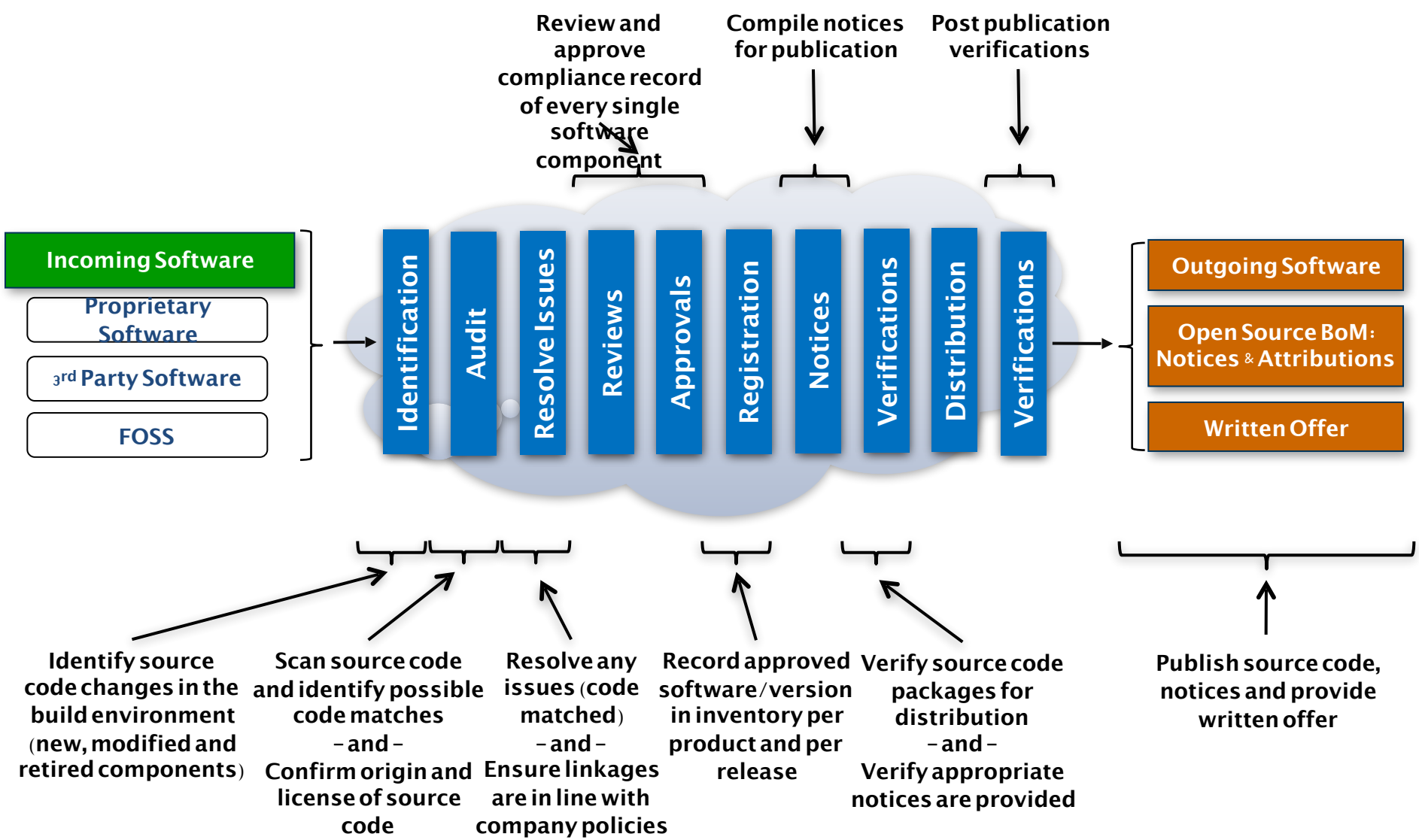
Science
(Systematic Approach)

Process

- **The way we ensure the policy is applied.**
- **Simple process:**
  - Check all incoming software
  - Identify origin, license, obligations, notices, etc.
  - Upon product release, meet the conditions of the licenses

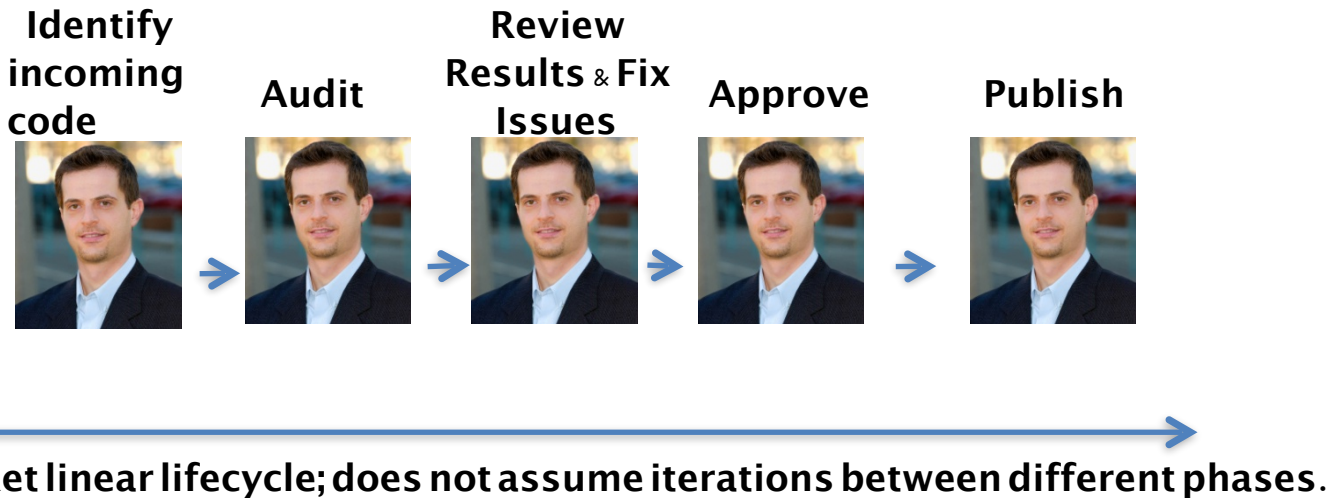


A More Complete Process

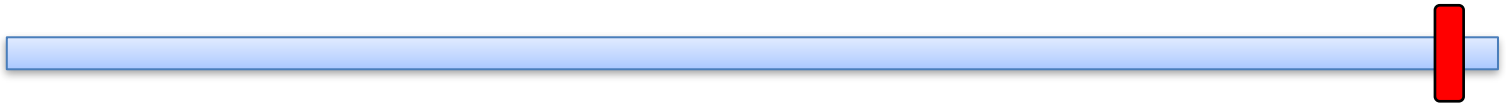


Process Story

- **What to do when you are understaffed?**
  - 1 JIRA ticket – 5 milestones in the JIRA process (identification, auditing, reviews, approval, fulfillment).



Process: Art / Science Meter



Art
(Creative Activity)

Science
(Systematic Approach)

Guidelines

- Guidelines to company's policy and process
- HOW-TOs
- Do's and Don't's
- License Compatibility Matrix
- License Playbooks
- Industry Best Practices
- Compliance 911

Guidelines Story 1

- **Comment found in source code while auditing it (circa 2008):**

> "I stole this code from <URL>"

Guidelines Stories 2 & 3

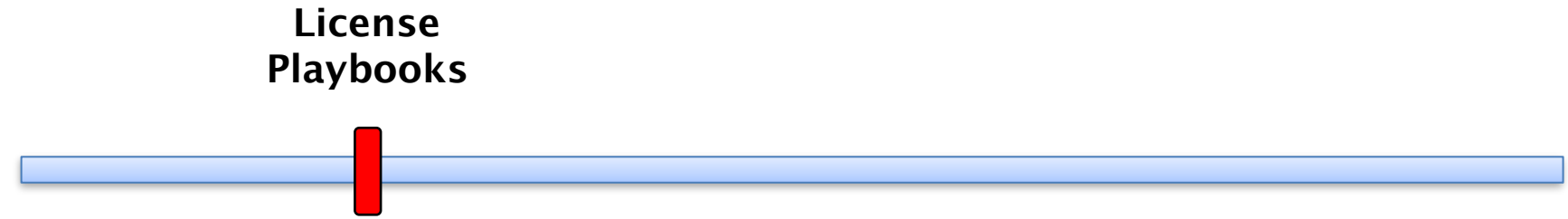
- A non-compliance issue found in source code comments:

  "In $Product_Code_Name, we are planning to eliminate this and replace it with code provided to us by $Company_Name_Chip_Vendor."

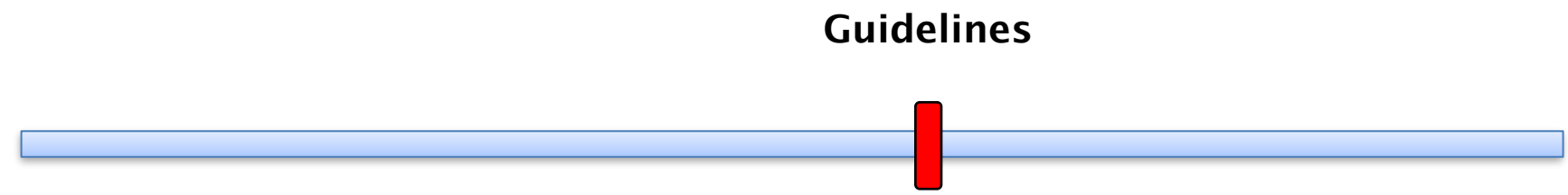
- A comment left by a QA Engineer (everyone is beyond stressed at this point)

  "This is still f------ broken [omitted]."

Guidelines: Art / Science Meter



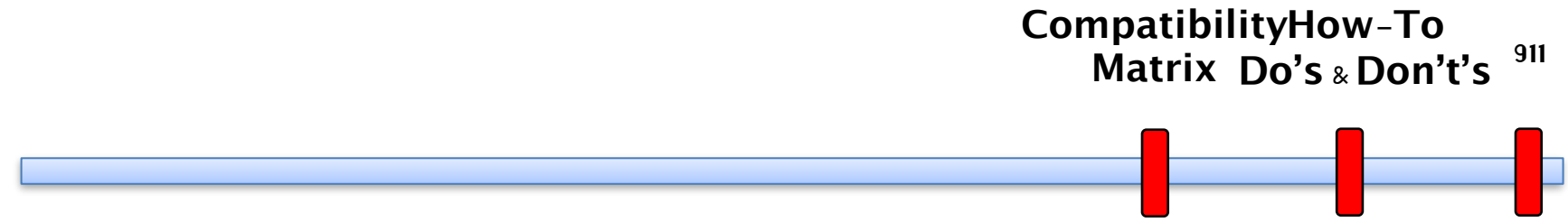
Guidelines: Art / Science Meter



Art
(Creative Activity)

Science
(Systematic Approach)

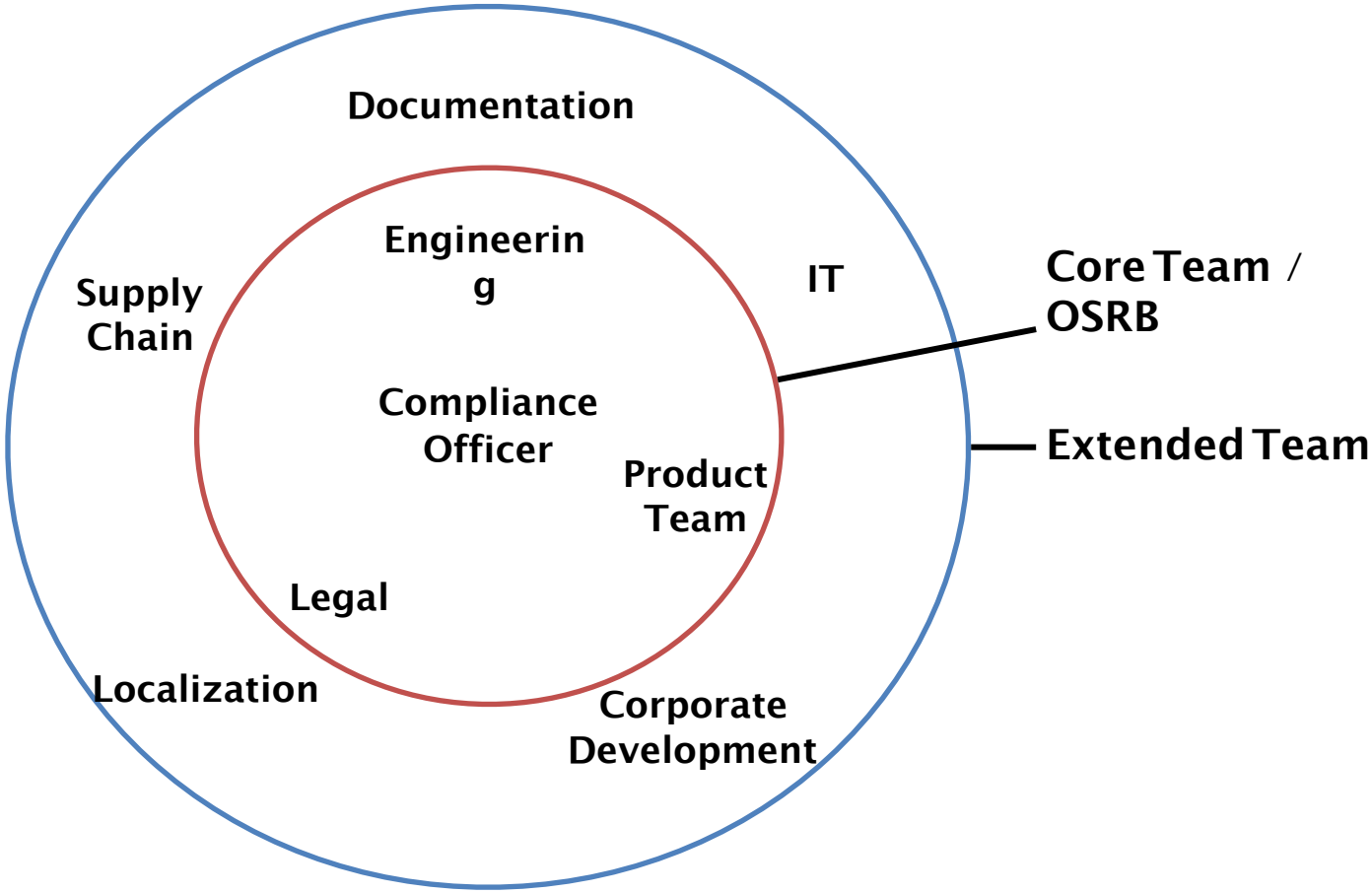
Guidelines: Art / Science Meter



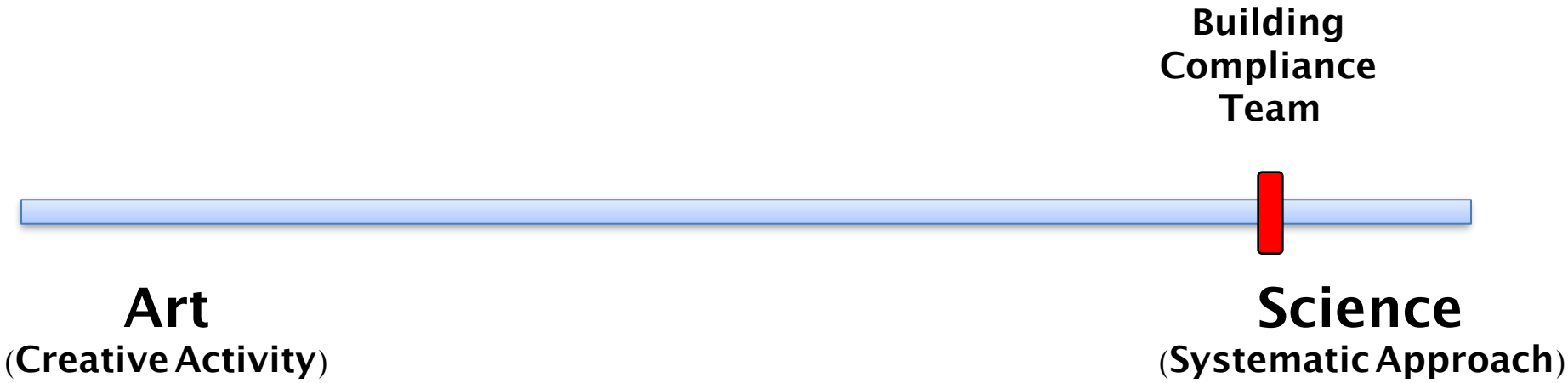
Art
(Creative Activity)

Science
(Systematic Approach)

Staffing



Staffing: Art / Science Meter



Staffing Story

Ibrahim, I am not convinced we need to do any of this compliance stuff and we need to transfer the compliance resources to development.

Training

- Crucial to the adoption of compliance.
- Internally and Externally provided and ranges from a brown bag lunch talk to a 2-days extensive workshop.

- STORY:

  Compliance Seminar #1 - Less than 10 people attended.

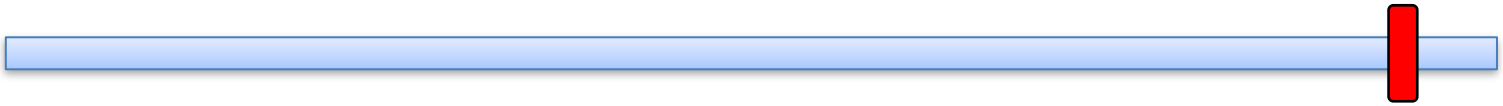
  Compliance Seminar #2 – Full house (> 300 developers)

Any guess on what influenced the attendance?

Audits and Tools

- **Tools**
  - Project management
  - Auditing
  - Linkage analysis

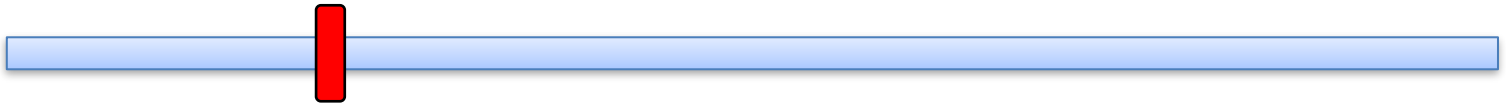
Running the Audits



Art
(Creative Activity)

Science
(Systematic Approach)

Interpreting the Audit Results



Art
(Creative Activity)

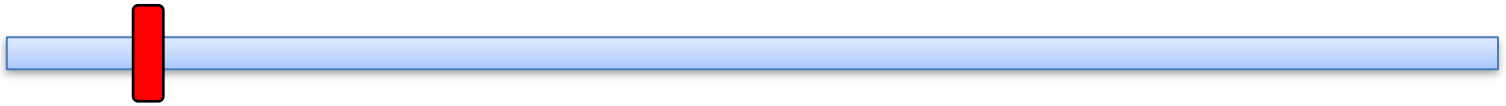
Science
(Systematic Approach)

Automation

- **We ship 100s of products every year, some with multiple firmware updates.**

- **How to deal with this industrial scale compliance?**

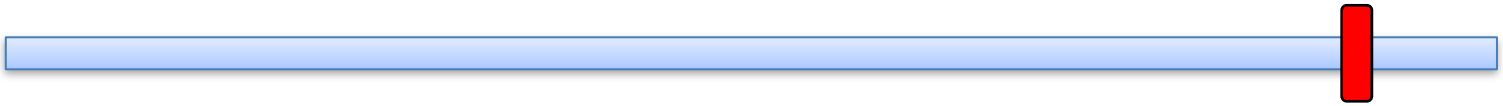
Coming up with a solution



Art
(Creative Activity)

Science
(Systematic Approach)

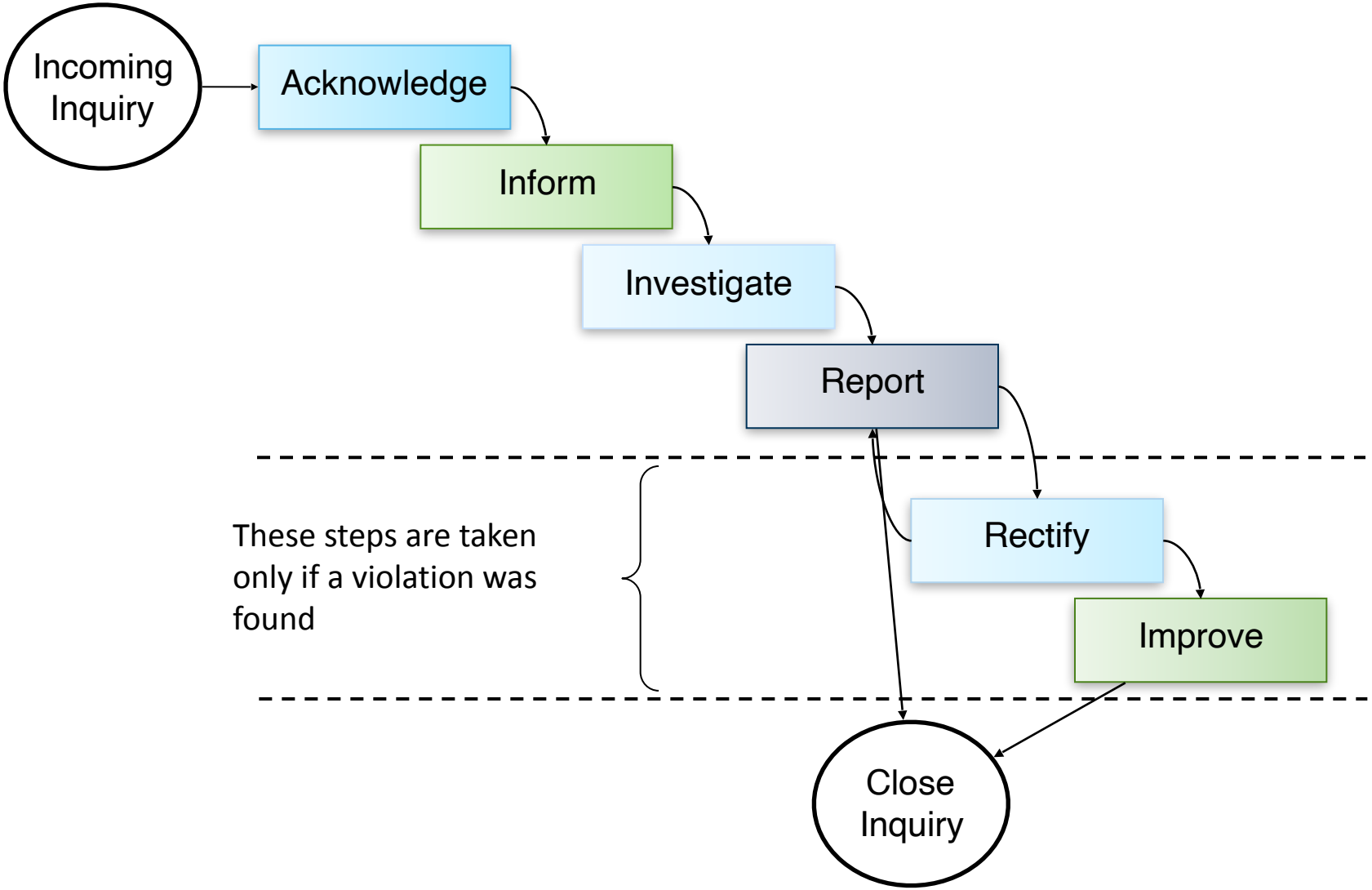
The Automation Solution



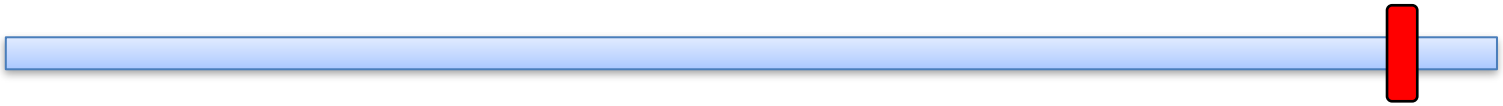
Art
(Creative Activity)

Science
(Systematic Approach)

Inquiries / Challenges



Managing Inquiries – Process



Art
(Creative Activity)

Science
(Systematic Approach)

Been there, done that!

Busted for Dodging Linux License, Samsung Makes Nice With Free Code

BY ROBERT MCMILLAN 08.20.13 | 6:30 AM | PERMALINK

Art
(Creative Activity)

Science
(Systematic Approach)

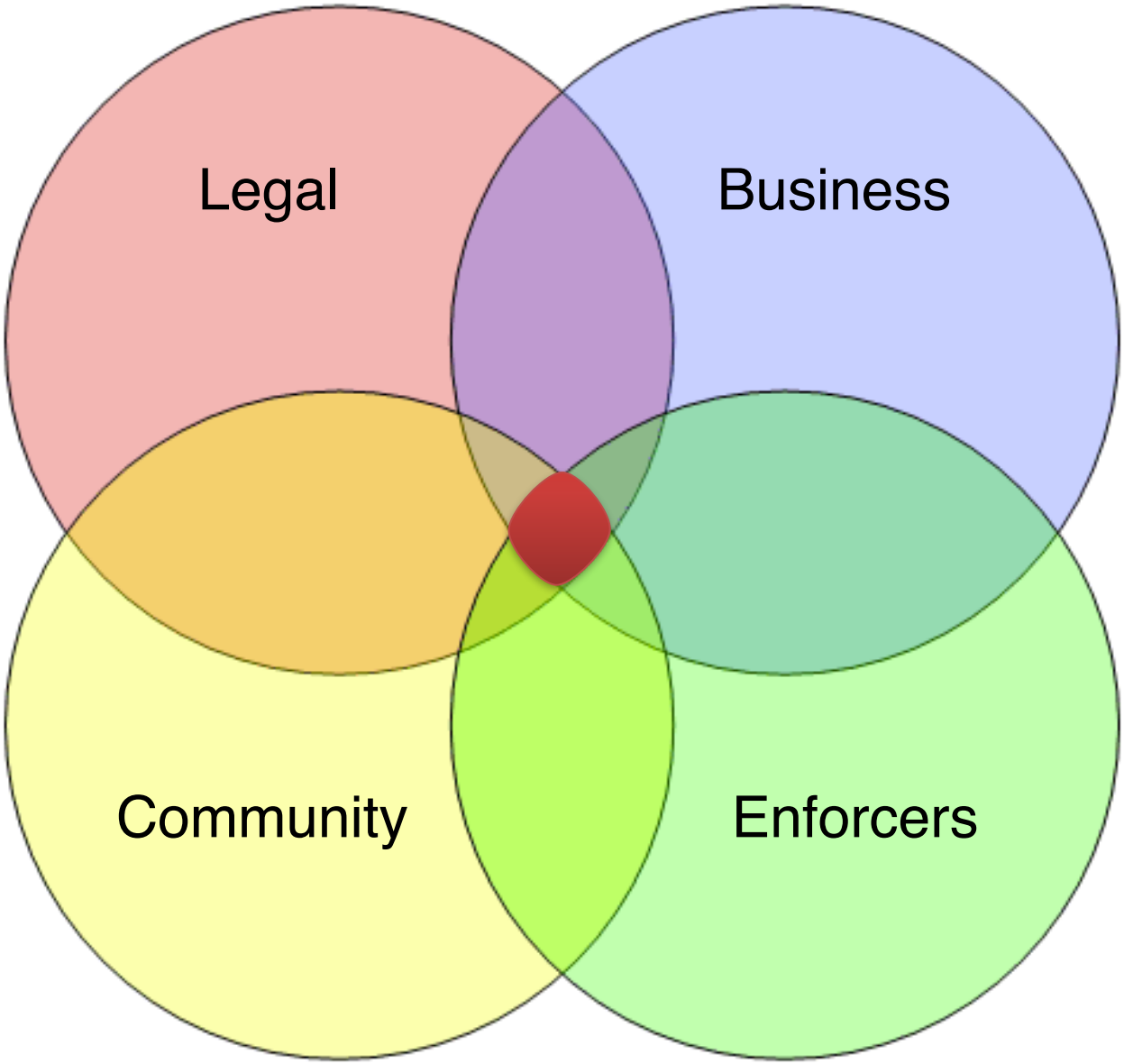
Closing

Balancing what?

- Internal & External Legal Counsel opinions / requirements
- Business needs (i.e. Ship product on time)
- Community needs (respect our work by respecting the license under which it is released)
- Enforcers, whistle blowers (we're watching you day-in and day-out)

It's easier to make enemies than to make friends.

Sweet Spot



Final Thoughts

- We've come a long way in compliance in the past decade and we learned a lot.
- Compliance is now more of a scalability and a cost issue, than a license debate and interpretation.
- The Next Frontier: How can we take cost out of compliance and provide a bullet proof approach that helps companies avoid compliance hiccups?

Top 3 interconnected challenge: Scaling, automation and cost.

Art or Science?

- It's a mix and the %s depend on who's looking and from which vantage point.

SAMSUNG
Open Source Group

We are hiring.

@SamsungOSG