



# Getting Started with Open Source Compliance

August 9, 2006



Holme Roberts & Owen LLP

*Attorneys at Law*

[www.hro.com](http://www.hro.com)

Denver Boulder Colorado Springs London Los Angeles Munich Salt Lake City San Francisco



---

**Where to begin?**



---

# **Understanding open source**

# Understanding Open Source

---

**Open source software is  
different from proprietary software**

# Understanding Open Source

---

“[T]he acquisition and use of FOSS necessitates implementation of unique risk management practices.”



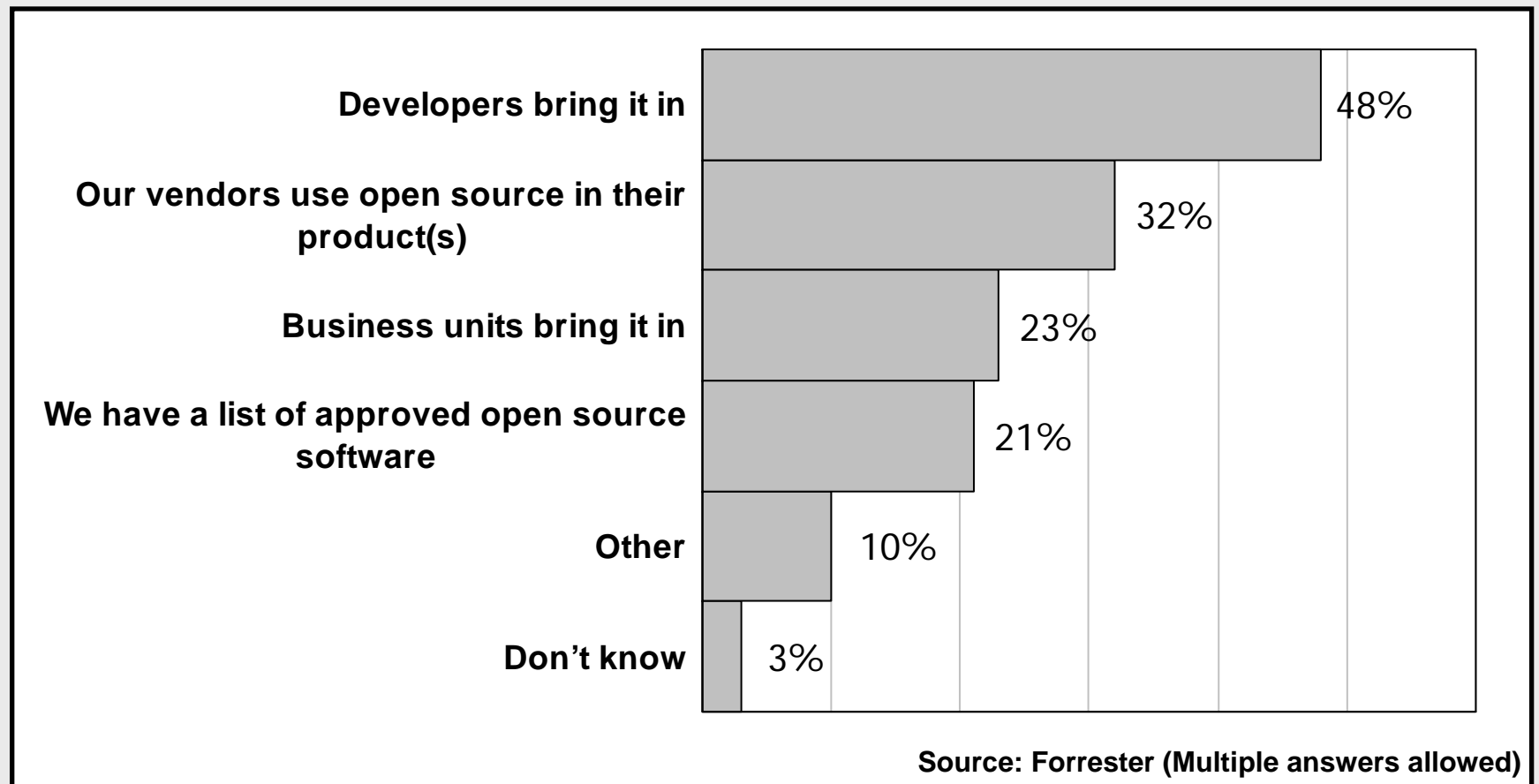
# Understanding Open Source

---

What do these  
**differences** can mean  
in terms of **compliance**?

# Understanding Open Source

## Open Source Procurement



# Understanding Open Source

---

**Open source software**

---

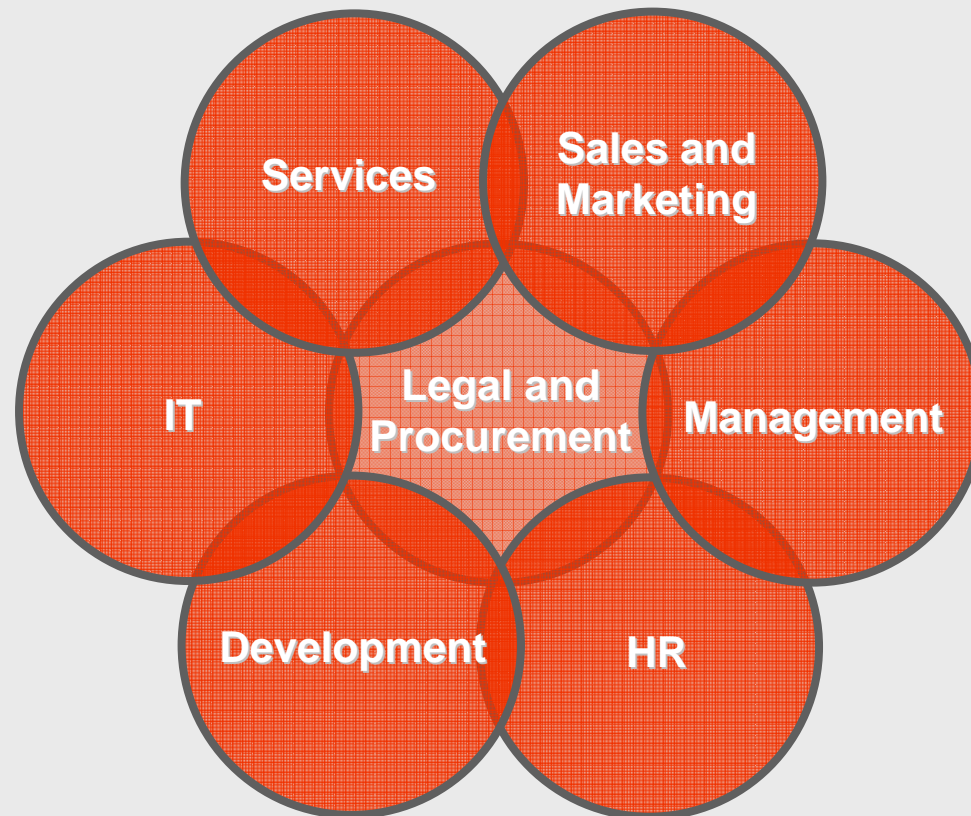
***Developer as gatekeeper***



# Understanding Open Source

## Cross-disciplinary Compliance

- Interdependent, not subservient
- Increased requirements for on collaboration and communication



# Understanding Open Source

---

**Open source software is also  
similar to proprietary software**

# Understanding Open Source

---

Open source software is  
**just software**

# Understanding Open Source

---

**Open source licenses  
make the software  
“open source”**

# Understanding Open Source

## Open Source Licenses Differ

Liberal

Copyleft

### No Strings

- MIT/X
- W3C

### Strings Attached

- *Original BSD*
- *Apache Software License*
- *Eclipse Public License*

### “Traditional” Copyleft

- GNU GPL
- GNU LGPL

### Additional Clauses

- GNU GPL v3
- *Common Public License*
- *Mozilla Public License*
- SISSL
- *IBM Public License*

# Understanding Open Source

---

Open source licenses  
are *enforced*

# Understanding Open Source

---

License analysis is  
*only one component*  
of compliance

# Understanding Open Source

---

**Compliance is about  
*managing risk* and  
*capturing benefits***



# Understanding the Risk

---

**The use of any software  
creates risk**

# Understanding the Risk

---

**The issue is not risk**  

---

***but, how much risk***

# Understanding the Risk

---

**Compliance requires  
understanding *your*  
potential open source risk**

# Understanding the Risk

---

What are some of the  
**potential risks?**

# Understanding the Risk

---

**Breach of contract lawsuits?**

# Understanding the Risk

---



**Not many. . .**



# Understanding the Risk

---

**Injunctions?**

# Understanding the Risk

---

**Not in this country. . .**



# Understanding the Risk



Let's save the GNU!

[gpl-violations.org](http://gpl-violations.org)



# Understanding the Risk

---

**Private enforcement actions?**

# Understanding the Risk



**>100 to date**

# Understanding the Risk

---

**Patent infringement lawsuits?**

# Understanding the Risk

---



v.



# Understanding the Risk

---

**Open source is also  
a diligence concern for:**

**customers**

**business partners**

**financing sources**

**acquirors**

# Understanding the Risk

---

**All open source risks**  

---

**are not created equal**

# Understanding the Risk

---

**Your risk depends on  
your use of open source**



# Understanding Compliance

---

Compliance requires  
*understanding*  
your use of open source

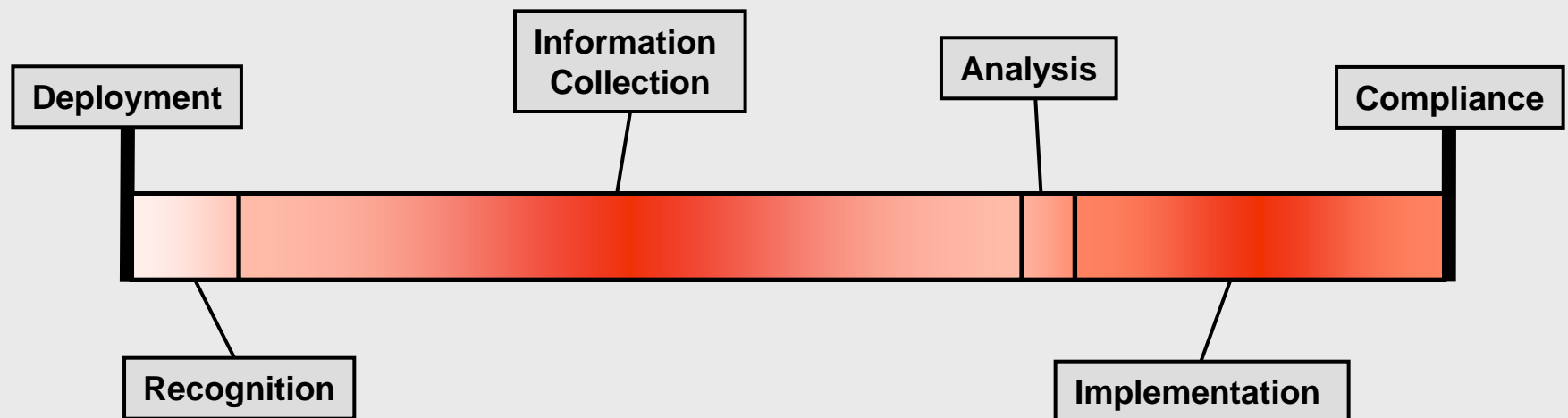
# Understanding Compliance

---

**The compliance process should  
drive this understanding**

# Understanding Compliance

## Compliance Process



- Increasing recognition of the need for compliance
- License analysis is also increasingly more manageable
- Beware of the practical bottlenecks
  - Information collection
  - Compliance implementation

# Understanding Compliance

---

Initial information collection  
is often handled through  
an **open source audit**

# Understanding Compliance

---

## Open Source Audits

- Understand and evaluate the scope and nature of your open source use
- Start with the open source software
  - Project name (and vendor)
  - Version/release number
  - Copyright owner(s)/sponsors of the project
- Understand the license
  - Name of license
  - Copy of license
  - Location of license in the code

# Understanding Compliance

---

## Open Source Audits

- Evaluate the use case
  - The nature of use
    - Internal or distributed
      - Where and how
      - Relevant product and business units
    - Modified or unmodified
  - Any interaction with other code
    - Proprietary
    - Open source
- Understand how the use may change over time

# Understanding Compliance

---

## Open Source Audits

- In practice, audits are not the perfect solution
  - Resource intensive
  - Cost intensive
  - Time consuming
  - Questionable accuracy
- Provide a snapshot, not an ongoing solution
- Use as part of an overall ongoing compliance program
- Avoid “management through audit”

# Understanding Compliance

---

**Best results start with**  
**clear objectives and strategy**



# Understanding Compliance

---

*What do you want  
from “compliance”?*

# Understanding Compliance

---

*Absolute*  
*compliance?*

---

*Consistent and reasonable*  
*standard of care?*

# Understanding Compliance

---

Define an  
**open source policy**

---

Develop specific  
**procedures and controls**  
to implement the policy

# Understanding Compliance

---

## Open Source Policy

- Begin with the open source policy
- Higher level
- Cover objectives and strategy
  - What does the Company hope to achieve/avoid by using open source?
  - What is the Company's commitment to open source?
- Conform to other corporate policies and corporate culture

# Understanding Compliance

---

## Open Source Procedures and Controls

- Develop procedures and controls to implement the open source policy
  - Case specific
  - Bright-line rules to guide specific uses (if possible)
- Emphasis on consistency
- Document the policy
- Circulate and centralize

# Understanding Compliance

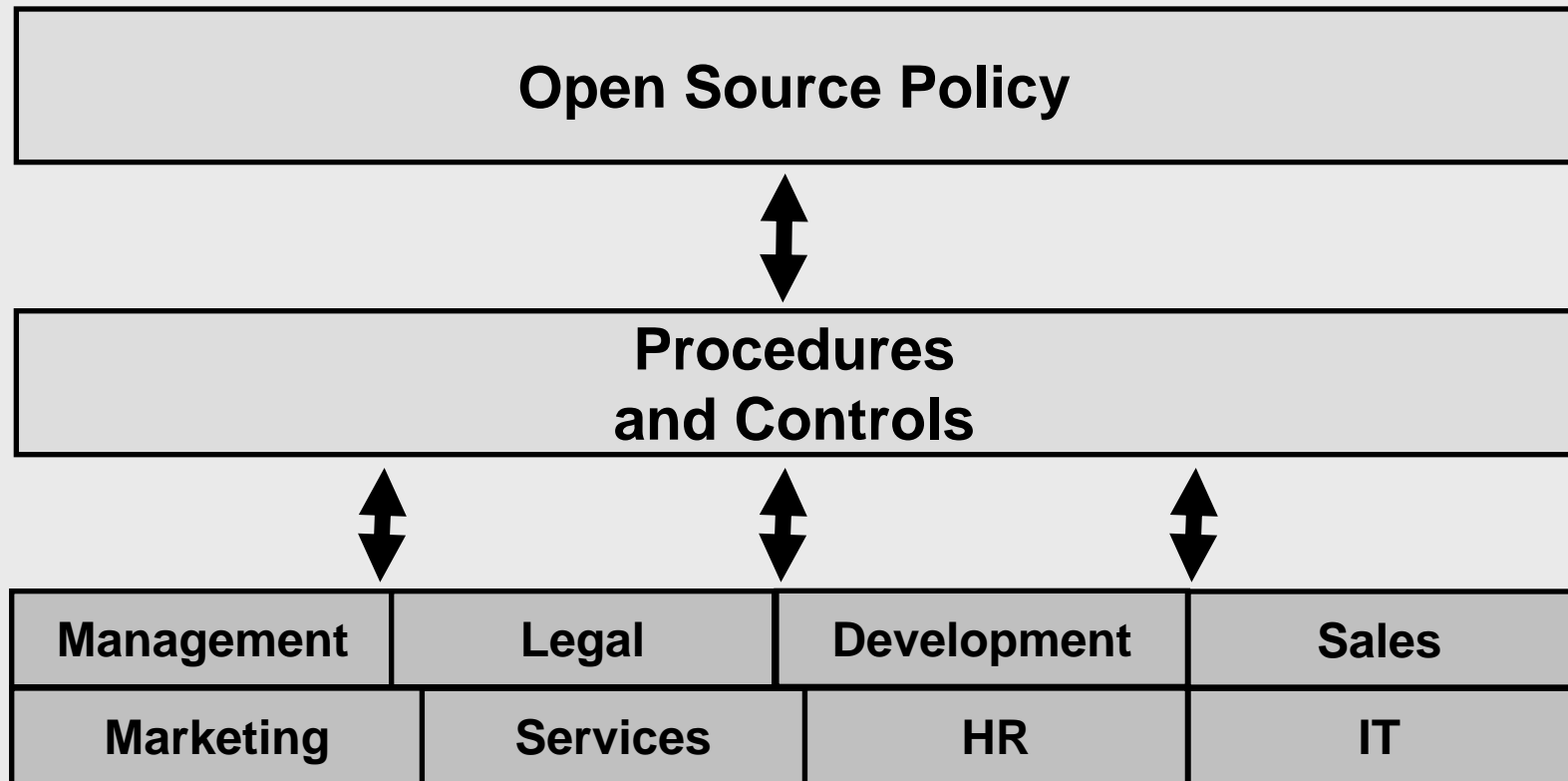
---

## Open Source Procedures and Controls

- Start simple and cover the basics
  - What requirements must be met before open source can be used within the Company?
  - What information must be collected in connection with open source usage?
  - Who will have responsibility for compliance?
  - Who will be the authority for open source decisions within the Company?
  - What procedures will be used to confirm and document compliance?
  - Will employees be allowed to contribute developments to open source projects and under what conditions?
  - Will the Company entertain publishing any of its software using an open source license?
- Add procedures and controls as your use and experience grows

# Understanding Compliance

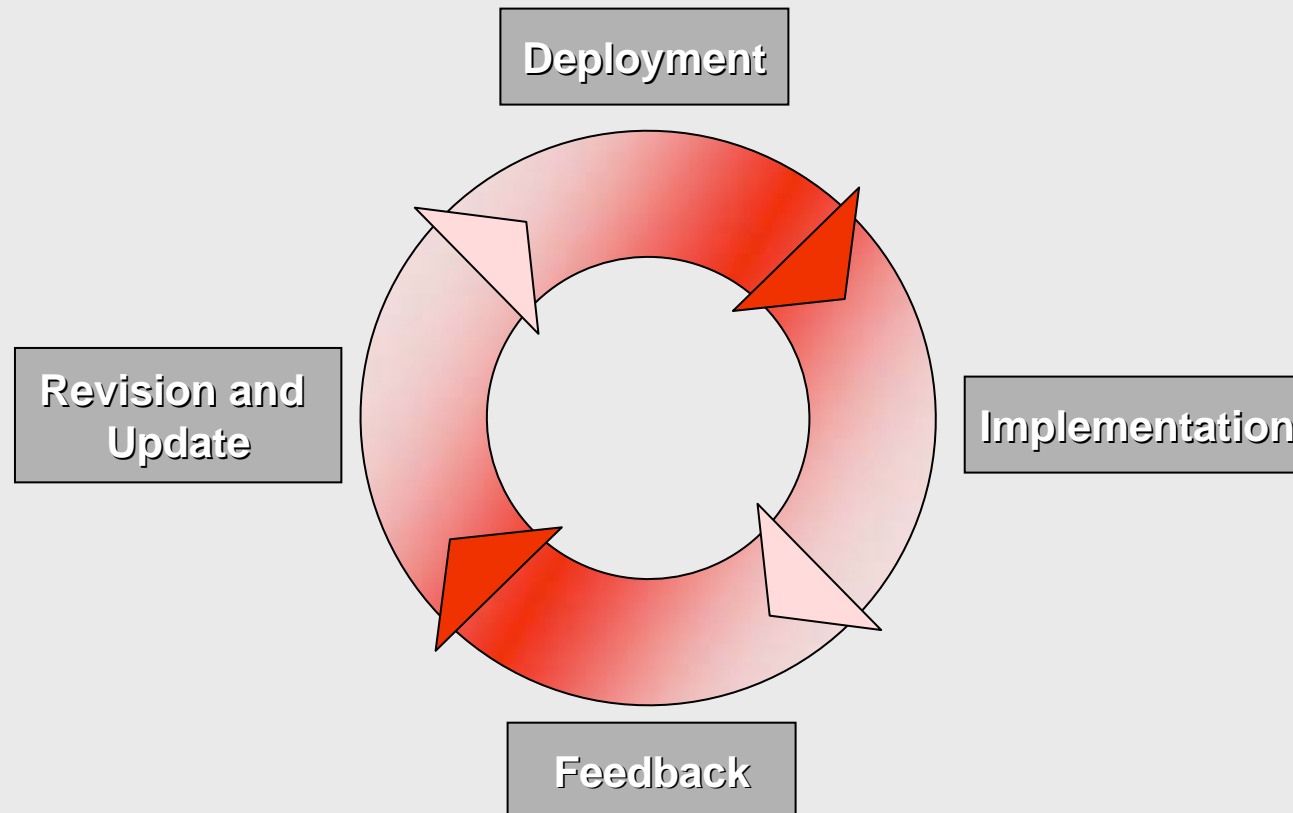
## Policy, Procedures, and Controls



# Understanding Compliance

## Ongoing Compliance Requires Communication

- Cultivate an internal open source “community” to provide feedback
- Allow procedures and controls to evolve over time





# Understanding Compliance

---

## Utilize Available Tools

- Infrastructure and support is now often similar to that found in the proprietary software world
  - Communication
    - Intranets
    - E-rooms
  - Legal
    - License analysis
    - Indemnification
    - Insurance
  - Managerial
    - Training
    - Consulting
    - Education
  - Technical
    - Platforms for implementation and management
    - Automated source code reviews
  - Operational
    - Support
    - Maintenance
    - Code updates

# Compliance Best Practices

---

## Key Recommendations

- Remember, compliance takes time
- Field a cross-disciplinary team
- Define objectives and strategy
- Develop a policy to fit the objectives
- Clearly document procedures and controls
- Keep it simple (and consistent)
- Operate in real-time (avoid reliance on audits)
- Review and evolve the program over time



---

# Software, Stacks and Support to Manage Open Source in the Enterprise

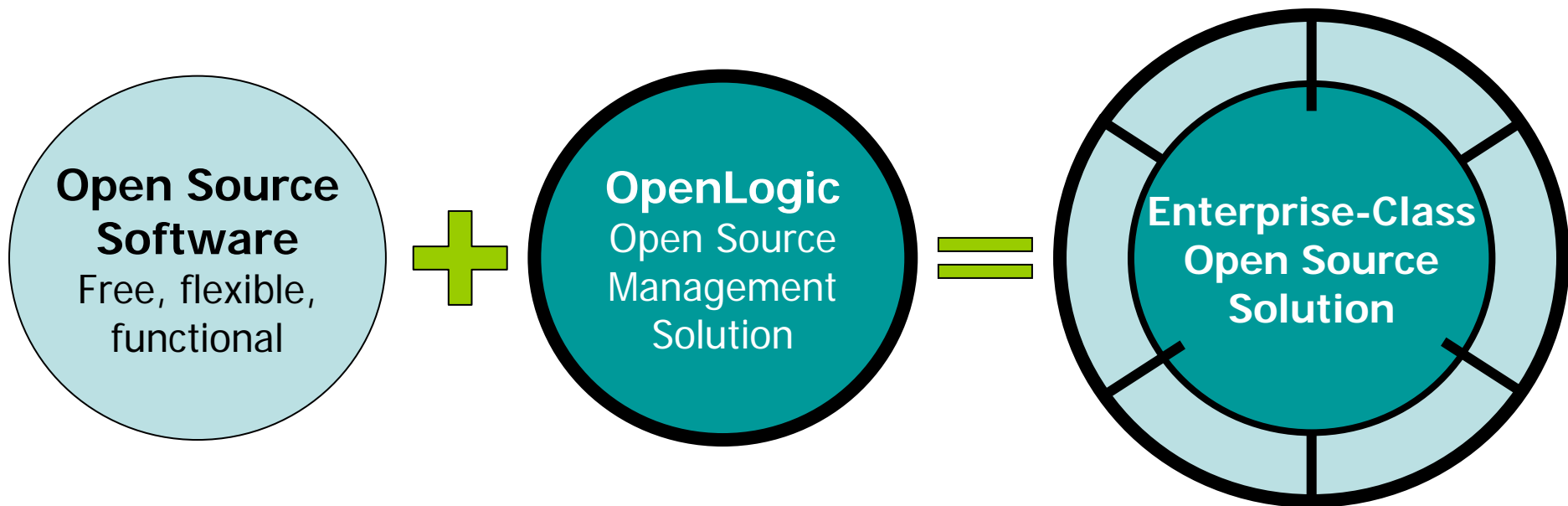
Webinar: Getting Started with Open  
Source Compliance

August 9, 2006

# Open Source Challenges

- **Selection Overload; Sourcing Uncertainty**
  - 100,000+ products; Can I depend on it?
- **Productivity Drains**
  - Time and effort to install, configure, integrate and test
  - Complexity of managing 5-7 new versions per open source product each year
- **Significant Legal & Compliance Risks**
  - Licensing, certification, policy enforcement
- **Support & Maintenance Issues Surface**
  - Companies want “One Throat to Choke”
  - Only a handful of open source products have commercial support

# Bridging the Gap



Unknown risk  
Hidden costs  
Inconsistent support

Certified Open Source Library  
Management Platform  
Technical Support

Reduced risk  
Lower TCO  
Consolidated support

# The OpenLogic Solution

OpenLogic Enterprise

OpenLogic  
Services

OpenLogic  
Management  
Suite

OpenLogic  
Knowledgebase

OpenLogic  
Certified  
Library

OpenUpdate Subscription

Certified Projects/Stacks

Your Software

Flexible Stacks



Open Source Made Easy

©2004 OPENLOGIC, INC. - COMPANY CONFIDENTIAL

# OpenLogic Certified Library: Breadth and Choice

Category	Selected Products
Web/App Servers	Apache, JBoss, Tomcat, Geronimo
App Frameworks	Castor, Hibernate, J2EE, Middlegen, Spring
Database	MySQL, PostgreSQL, DB2 connector, Oracle connector
IDE	Eclipse, Eclipse plug-ins, JEdit, NetBeans
Source Code Control	CVS, WinCVS, Subversion
Builder	Ant, Maven
Web Frameworks	JSF, SpringMVC, Struts, Tapestry, Webwork
Java Utilities	ANTLR, AspectJ, Jakarta Commons, JMeter
XML	Castor, Docbook, Xalan, Xerces
Testing	DBUnit, HttpUnit, JUnit, JWebUnit, struts testcase
Language	Java, PHP, Python, Perl
Visual	Cewolf, GraphViz, JFree Chart



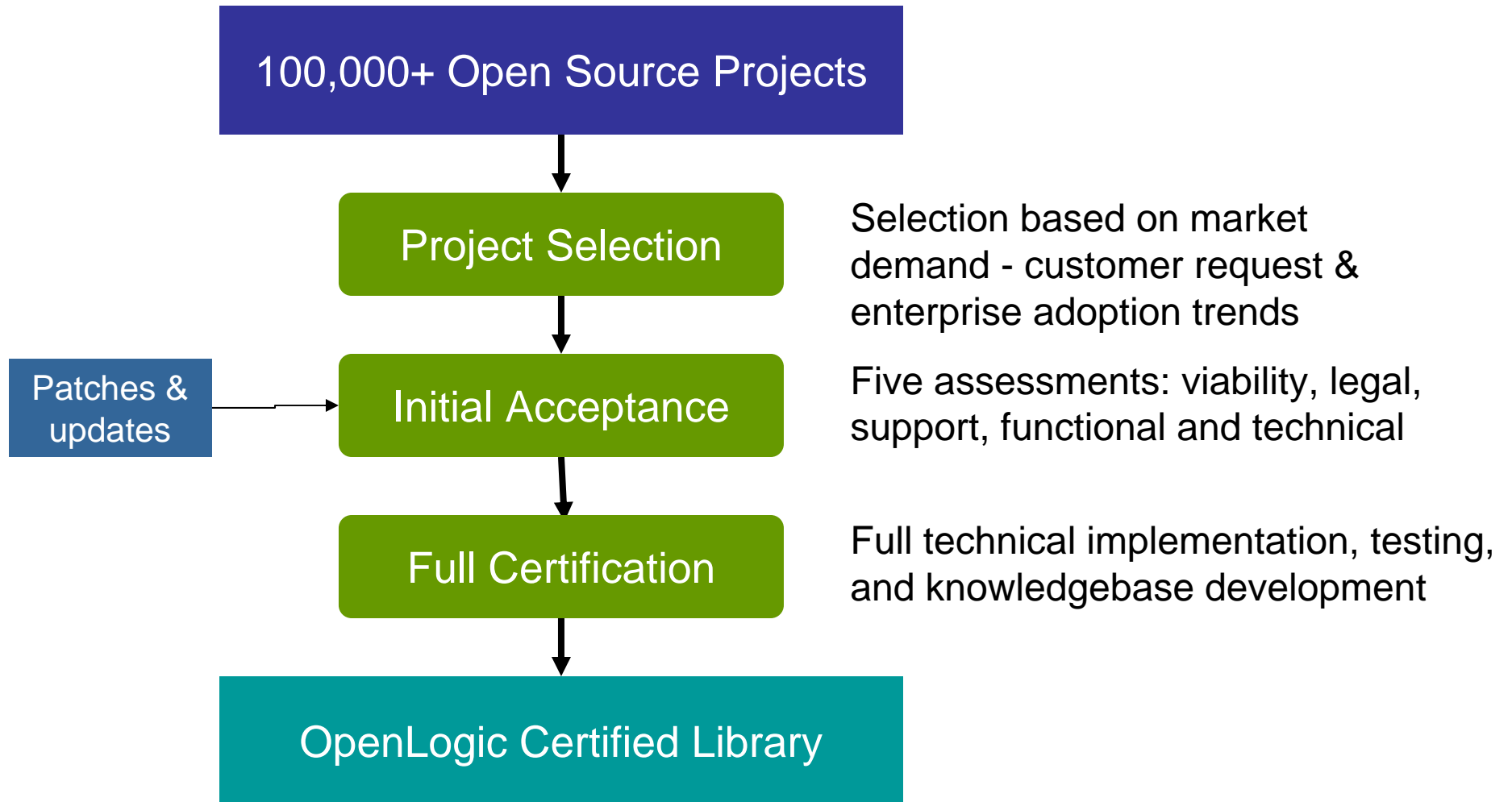
Struts



Open Source Made Easy

©2004 OPENLOGIC, INC. - COMPANY CONFIDENTIAL

# How We Certify





# The OpenLogic Solution

OpenLogic Enterprise

OpenLogic  
Services

OpenLogic  
Management  
Suite

OpenLogic  
Knowledgebase

OpenLogic  
Certified  
Library

Licensing Info

Dependencies

Configuration

Integration

Documentation

Sample Apps

OpenUpdate Subscription

Certified Projects/Stacks

Your Software

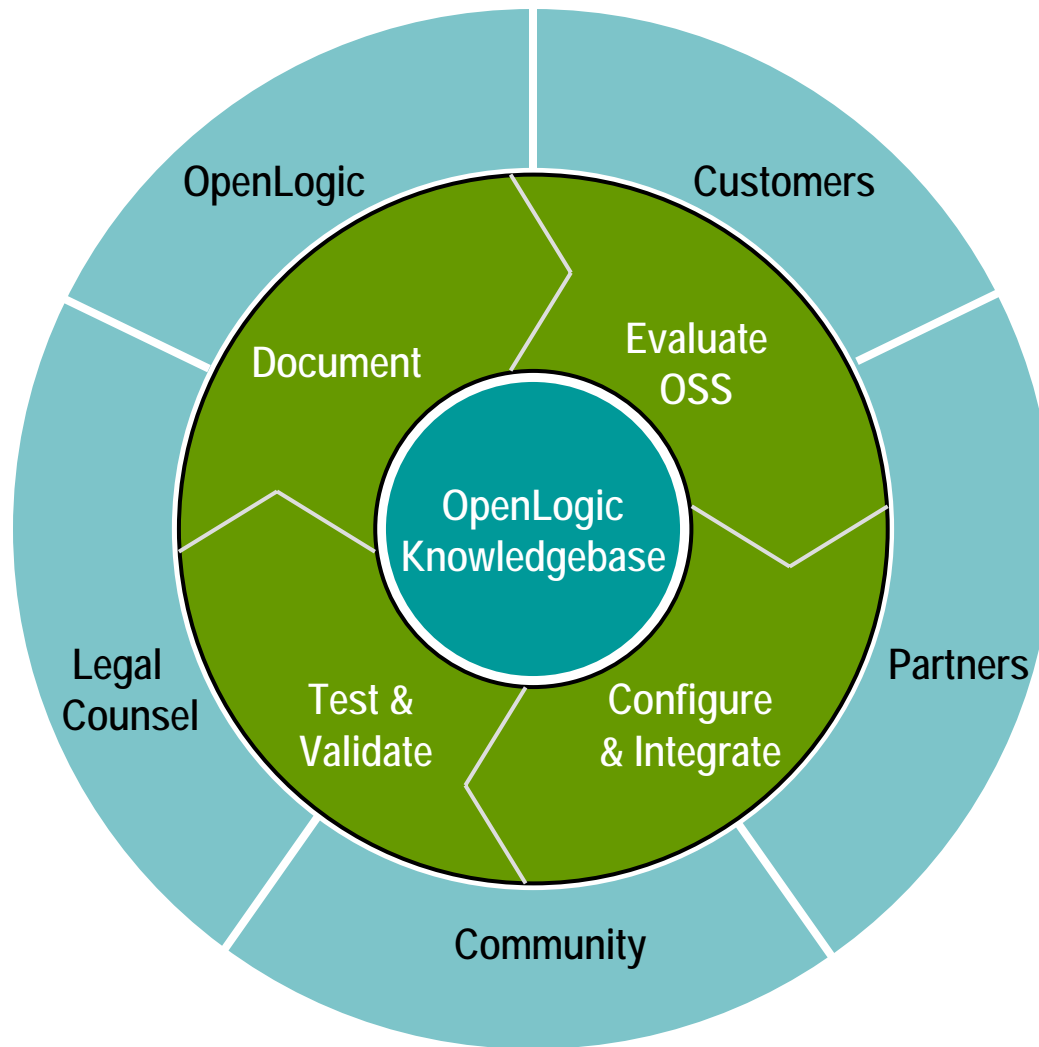
Flexible Stacks



Open Source Made Easy

©2004 OPENLOGIC, INC. - COMPANY CONFIDENTIAL

# Knowledgebase: The Collaborative Effect



Stakeholders

Certification Process

# The OpenLogic Solution

OpenLogic Enterprise

OpenLogic  
Services

OpenLogic  
Management  
Suite

OpenLogic  
Knowledgebase

OpenLogic  
Certified  
Library

Enterprise Control  
Enforce open source policies

Technical Staff Productivity  
Automate open source rollout

Licensing Info

Dependencies

Configuration

Integration

Documentation

Sample Apps

OpenUpdate Subscription

Certified Projects/Stacks

Your Software

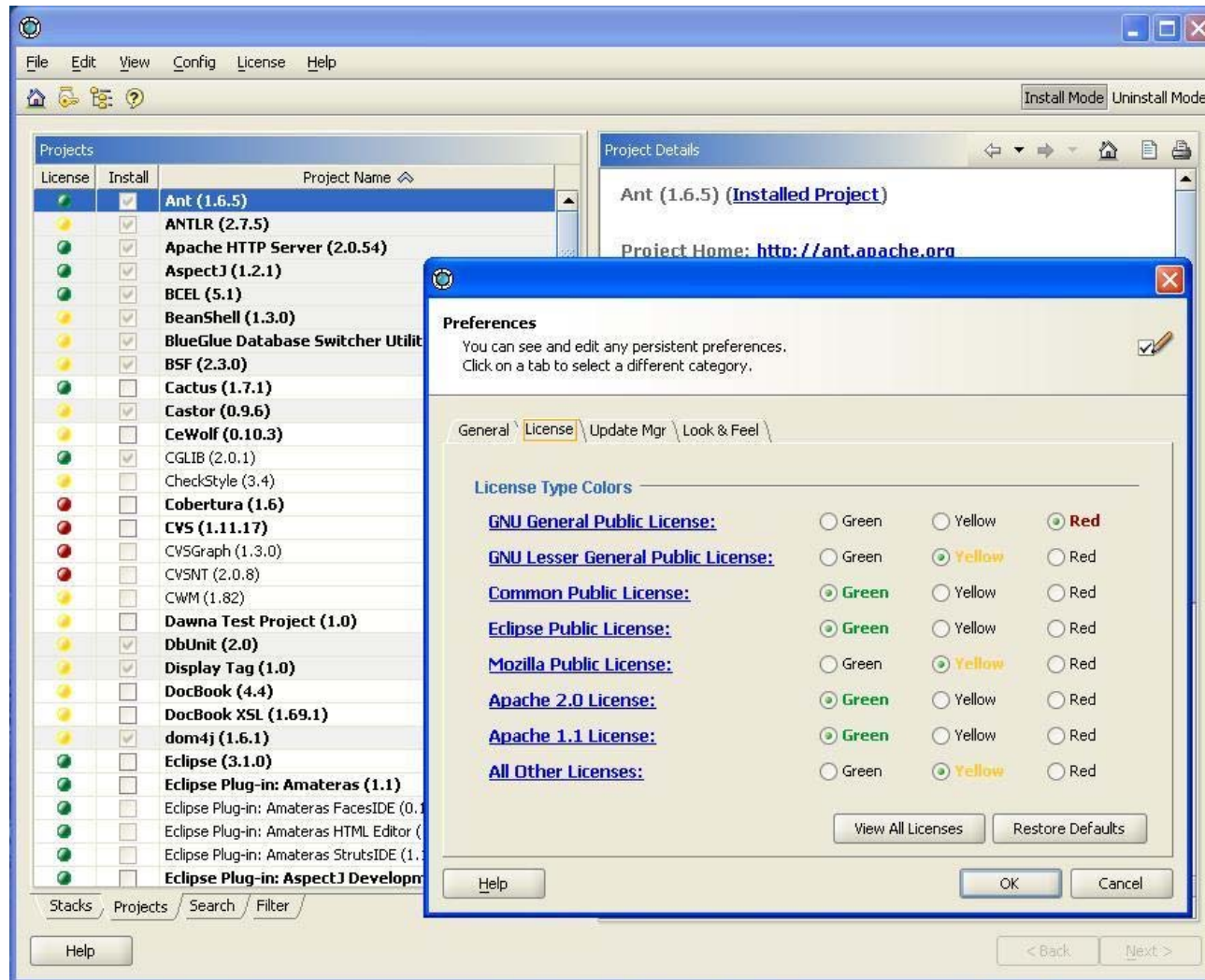
Flexible Stacks



Open Source Made Easy

©2004 OPENLOGIC, INC. - COMPANY CONFIDENTIAL

# Management Suite



# The OpenLogic Solution

OpenLogic Enterprise

OpenLogic  
Services

OpenLogic  
Management  
Suite

OpenLogic  
Knowledgebase

OpenLogic  
Certified  
Library

Consolidated  
Support

Custom  
Certification

Consulting  
& Training

Enterprise Control  
Enforce open source policies

Technical Staff Productivity  
Automate open source rollout

Licensing Info

Dependencies

Configuration

Integration

Documentation

Sample Apps

OpenUpdate Subscription

Certified Projects/Stacks

Your Software

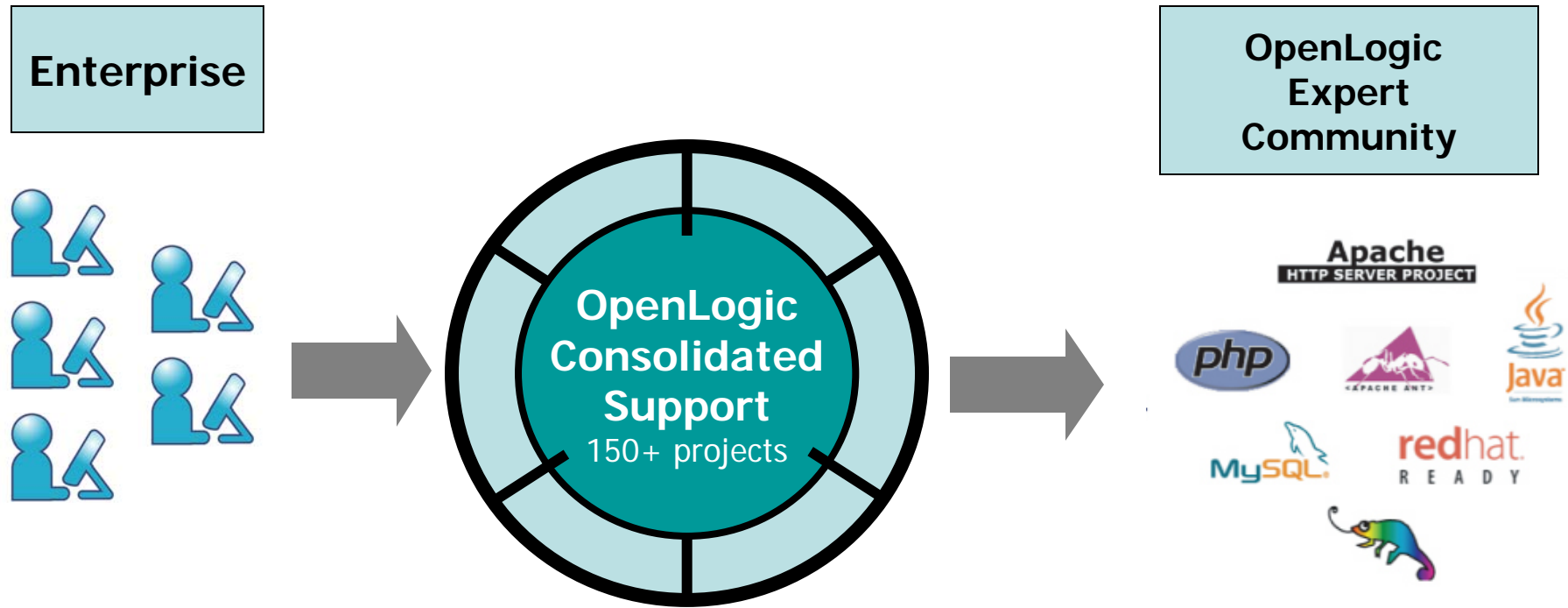
Flexible Stacks



Open Source Made Easy

©2004 OPENLOGIC, INC. - COMPANY CONFIDENTIAL

# OpenLogic Consolidated Support



# Support Service Levels

	Online	Business Hours	24x7
Hours	8 EST – 5 PST	8 EST – 5 PST	24x7
Problem Submission	Online	Phone/ Online	Phone/ Online
Response Time	8 Hour	4 Hour	2 Hour

# OpenLogic Offers Indemnification

- Which open source?
  - All certified open source in OpenLogic's library
  - Currently 160+ products
- What pre-requisites?
  - Must purchase OpenLogic Enterprise
  - Must purchase support for that particular open source product in order to get indemnification
- Cost?
  - No additional charge once the pre-requisites are met



# Wide Adoption, Proven Solution



Open Source Made Easy

# Contact Information

**Thank You.**

Please visit our website at [www.openlogic.com](http://www.openlogic.com)

Call us at **888-OpenLogic**

Send an email to:

[Mark.Winz@openlogic.com](mailto:Mark.Winz@openlogic.com)

[Jason.Haislmaier@hro.com](mailto:Jason.Haislmaier@hro.com)



Open Source Made Easy

©2004 OPENLOGIC, INC. - COMPANY CONFIDENTIAL