Agenda

- Welcome and Introduction – Eran Strod
- Open Source Best Practices – Hal Hearst
- Questions & Answers
- Next Steps
About Black Duck Software

Accelerate time-to-market and reduce development costs by providing products and services for finding, managing and confidently deploying open source software.

Mission

Founded in 2002 and backed by industry leaders

Black Duck Global Distribution
Mixed Code Development Adds Risk

- Loss of Intellectual Property
- Export Regulations
- Security Vulnerabilities
- Software Defects
- Injunctions
- Contractual Obligations
- Escalating Support Costs
- License Rights and Restrictions
Speaker

Hal Hearst
Sr. Director of Professional Services
Black Duck Software

Background

- Responsible for delivering software assessment and implementation services to Black Duck Software’s customer base
- Help Black Duck customers design and implement processes to manage the use of open source software
- Been with Black Duck Software Since October 2004
- 20 year career in professional services with companies such as Accenture, SAP and others
Treat the management of open source software as an integrated, cross functional **business process**, and not simply as a development process.
Golden Rule Details

- **Cross functional**
  - Product Planning/Management
  - Legal, Security & Export Compliance
  - Engineering

- **Integrated Processes**
  - Component Management
  - License Management
  - Release Management
    - Release Planning
    - Release Delivery
  - Security Review
  - Export Compliance Review
Golden Rule Details - Continued

- **Systemic**
  - Baked in to the culture & workflow
  - Event Driven
    - Component approval request
    - Planning a release
    - Accepting a code drop from a vendor/outsourcer
    - Performing a build
    - Creating a release

- **Embrace Supply Chain Techniques**
  - ERP systems brought together different users and processes
  - Workflow automates task creation
    - Notifications
    - Process Monitoring
  - Central repositories of data
  - Business Process Integration is the key
Example Supply Chain Business Process

- Item Need Determined
- Purchase Req. Created
- Purchase Req. Approval
- Purchase Order Created & Sourced
- Item Arrives in Receiving
- Transfer Order and Inspection Order Created
- QA Inspects & Releases to Inventory
- Production Requests to use Items for Order
- Manufacturing
- Order Consumes the items

Planning

Procurement

Inventory Mgmt

Quality Control
Supply Chain Comparison

- Technology companies have software supply chains
- Software products have bill of materials (BOM’s)
- Tech. companies have similar roles and events
  - Materials Planner = Product Management
  - Purchase Req’s = Component Approval Request
  - Warehouse = Source Code Management / Asset Management
  - Quality Assurance = Numerous types of code analysis
  - Procurement Approvals = Legal & Compliance Approvals
  - Shop Floor Production = Engineering
Example Software Development Business Process

Innovation Happens, need for a component is identified.

Component Approval Request Created

New License initiates license review

License Approved with Conditions for Use

Conditional Approval Granted

Review Business Case, Support Options and other Criteria

Perform Risk Assessment, Security Reviews and Export Compliance Reviews

Domain Specific Review Boards

Engineering Mgmt

Engineering

Implements Component

Verifies Compliance for Release

Product Management

Copyright © 2008 Black Duck Software, Inc. All Rights Reserved.
Application Development Lifecycle
Supporting Open Source-based Development

Select
Code based on policies and key metadata

Search
For code to use within applications

Approve
Code based on organization’s control polices

Monitor
Code usage and impact across complex applications

Build
The approved code using preferred tools

Validate
That only authorized code is used
Black Duck’s Portfolio

Code Center

koders
powered by blackducksoftware

EMPOWER

Search
Select
Approve

CONTROL

Monitor

Validate

Build

Partner Integration

Protex
Export

Copyright © 2008 Black Duck Software, Inc. All Rights Reserved.
Open Source Programs Elements

1. Published Policy
   1. Created via Cross Functional Team
   2. Organization is educated on the policy

2. Open Source Process Owner
   1. Keeps the wheels running
   2. Grant certain types of approvals

3. Approval Processes
   1. Component Review & Approval
   2. License Review & Approval
   3. Release Plan Review & Approval

4. Monitoring & Tracking Process
   1. Component Verification
   2. Security Notifications
   3. Component Upgrade Notifications

5. Obligation Verification Process
   1. Ensure using approved components... and...
   2. Meeting the license and business obligations
Determine Policies

- **Software development supply chain management**
  - Open source, vendor, partner, contractor, outsourcers, other internal organizations, ...

- **Define criteria for approved software**
  - Licenses
  - Sources
  - Support
  - Other

- **Define criteria for unapproved software**

- **Define conditions for participating in the Open Source Software development**

- **Employee Education**
  - No compliance without education
Select a Compliance Core Team

- **Legal**
  - Perform iterative review of identified components

- **Open Source Process Owner**
  - Appoint a person with overall responsibility

- **Business / Product Perspective**
  - Prioritize products (by release) for analysis

- **Technical / Lead Architect**
  - Integrate analysis and review with the development process
  - Identify code based on automated discoveries

- **Project Management**
  - Coordinate resources
  - Drive the project plan
  - Resolve issues
Establish Process

- How development teams and other functions
  - Search, select, approve, track, validate, track & monitor

- Inbound approval processes
  - Code from internal teams, external sources

- Outbound compliance processes
  - Distributed code

- Create a Baseline
  - Prioritize
  - Perform code analysis
  - Plan remediation
  - Document the origins of the code base
  - Determine all components and licenses in use
  - Verify usage is approved
  - Create a catalogue of approved components and licenses

- Validation processes
Enterprise Collaboration

Off Site
- Outside Counsel
- Auditors
- Off-Shore Developers

On Site
- Developers
- Development Managers
- Open Source Review Board
- QA Review Board
- Security Review Board
- Legal Review Board
- Other Users

Web Application

Black Duck KnowledgeBase

Policies
Catalog Metadata
Global Rollouts Require a Project & Sponsor

Many methodologies work, but typically they have:
• Plan
• Design
• Implementation
• Rollout

May require a pilot and stakeholder approval:
• Global Process
• Implemented in Multiple Business Units
Implementation Deliverables and Phases

1. **Design Phase**
   - Identify server topology
   - Create deployment plan and articulate integration points
   - Define test plan

2. **Development Phase**
   - Deploy to pilot group
   - Customize the application and the reporting features
   - Present test results

3. **Deployment Phase**
   - Deploy client application to end-users
   - Connect external applications through integration points
   - Disseminate policies company wide

4. **Post-Deployment Phase**
   - Manage support issues
   - Poll end-user experience
Phased Deployment Plan

Depending upon need, you can designed phased deployment plans to quickly yield value

- Code Baseline
- Remediation Work
- Ongoing Analysis
- Hardware Topology
  - Scaling across sites, users, products
- Training
  - Technical, legal
- Policies, Process, and Resource Definition

Quick way to yield value
Audit what you have to help determine policies
Effective Management of Components

Leverage OSS / 3rd Party Code

Acquire SW

Find Code

Catalog

Search & Select | Approve | Track

Build

Release

Approved BOM

Validate

Identify OSS / 3rd Party Code

Protex

Export

Identify Encryption
The Black Duck KnowledgeBase

Product Portfolio Foundation

Comprehensive open source database
- 170,000+ OSS projects
- From 3,600+ sites
- Spanning 560+ million files
- Tens of billions of lines of code
- Released under 1,400+ unique licenses
- 31,000+ security vulnerabilities

Extensive metadata
- Name, description, versions, URL
- License, programming language, OS
- National Vulnerability Database
- Cryptography
- Code Prints of source/binary
- Other information

- Continuously expanded
- Custom Code Printing to add proprietary code
- Daily security vulnerability alerts
- Updates issued 1-2 times per month
Black Duck Professional Services

Deployment Services
Enablement Driven
- Software Implementation Services
- Strategic Planning
- Project Implementation
- Custom Development
- Training
- Integration

Assessment Services
Event Driven
- M&A Due Diligence
- Funding Event
- OEM Agreement
- Internal Audit
- Vendor Assessment

GOAL
Customer Success

GOAL
Help Evaluate Risk
Assessment Services

- Short-term engagements
- On-site or remote analysis
- Work with a variety of security, confidentiality and privilege requirements
- Report based
  - Executive Summary
  - Detailed Discoveries
  - Potential Risks, Conflicts
- Service is embedded in several customer’s (M&A / OEM) processes
Put Black Duck Software to Work

- Accelerating software development by enabling you to better leverage open source
- Helping you avoid the pitfalls of mixed code development
- Managing your open source approval process
- Revealing the unknowns in your software

Know Your Code™
Questions and Answers
Next Steps

- Black Duck Knowledge Center
  http://www.blackducksoftware.com/resources

- Black Duck Open Source License Resource Center
  http://www.blackducksoftware.com/oss

- For more information, email: info@blackducksoftware.com
Thank You for Attending