organizational participation in
open communities

PARTICIPATION WITH OPEN SOURCE COMMUNITIES:

REFRESHER and MATURITY MODELS

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

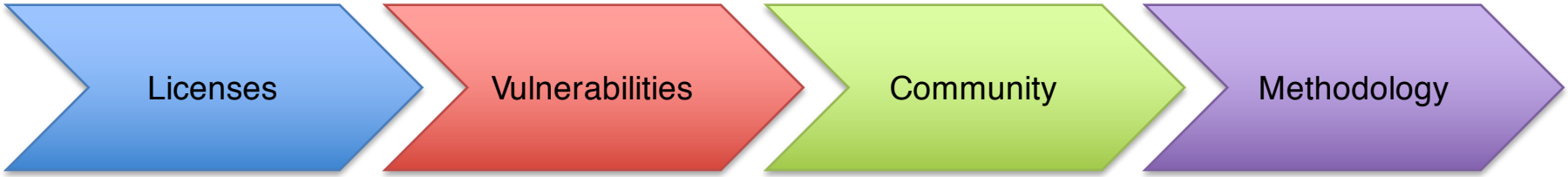
The Future of Open Source 2016

- > 65% use open source to speed application development
- > 55% use open source for production infrastructure
- Top issues for engaging open source
  - Operating Systems
  - Database
  - Software Development Lifecycle
- 58% are reviewing open source only under special circumstances

- https://www.blackducksoftware.com/2016-future-of-open-source

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

Open Source Software is Four Things



- The business model shifts to contribution and support
- The more you get involved, the more you can influence/control
- If you don't understand the licensing, you may expose proprietary information
- Vulnerabilities are important even when software isn't shipped downstream

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

organizational participation in open communities

Open Source Software Licenses

Licenses

- Nearly 90 licenses today as recognized by OSI
- Two basic types of licenses
  - Reciprocal licenses that require code changes to be returned to the community at large. This type of license is also called a Copyleft license.
  - Licenses that permit modified versions to be retained as proprietary and permit arbitrary integration into proprietary software. This type of license is also called a Permissive license.

Copyrights are still a core foundational element of all Open Source licenses

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

organizational participation in open communities

Open Source Software Vulnerabilities

Vulnerabilities

- NIST Provides a database of published vulnerabilities
  - There are open source initiatives to identify, publish, and distributed known vulnerabilities associated with open source software.
  - One-third of companies have no process for identifying and tracking or remediating known open source vulnerabilities
    - 10th Annual Future of Open Source Survey – Black Duck Software

Vulnerabilities are found throughout open source software

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Open Source Community

Community

- Any collection of developers with a common interest
- Historically made up of free agents
- Increasingly funded by large companies sharing development costs
- Governments and academia also contributing at an increasing pace
- Membership & “rank” within community based on individual’s reputation
- Corporate reputation plays a significant, yet secondary role

Open Source Communities are a meritocracy in the sense that reputation and influence are measured by sustained individual contributions rather than corporate directives.

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION’S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Open Source Methodology

Methodology

- Communal, shared development
- Various projects each with their own subculture
- Very few roadmaps, but some projects are starting to publish them
- Influence and control is achieved by being involved
- Individuals are largely in control, not companies

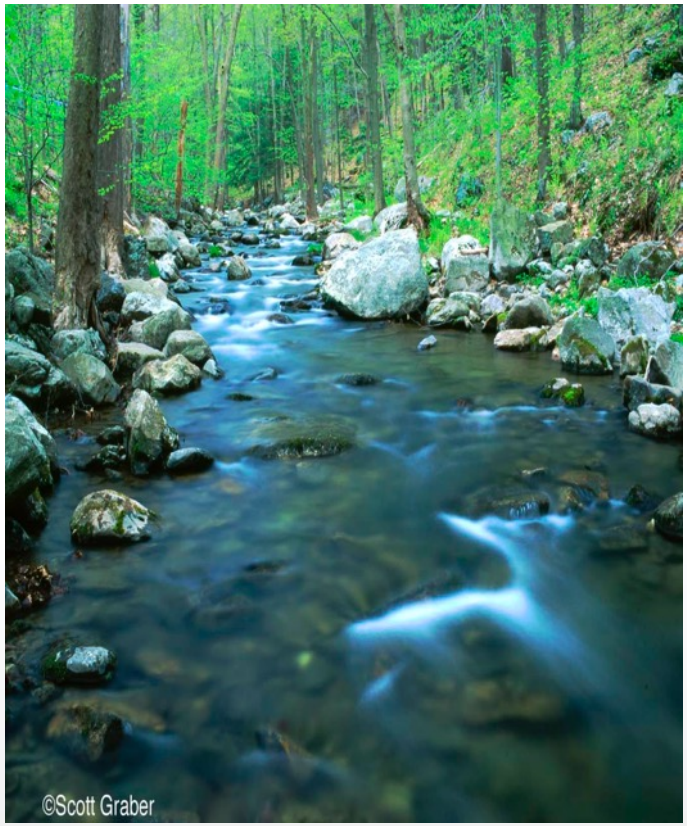
Governance models vary widely,
some autocratic, others consensus based

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Open Source is Like a Natural Resource

- Think of Open Source as a “commons” of code similar to a natural resource
- Any Open Source project requires an ecosystem to survive
- Many businesses utilize the “commons” to bring products to market in some way
- Businesses that try to take without concern for the overall ecosystem get repelled by others
  - Organizations exist for the sole purpose of protecting the commons (such as SFLC, OSI, FSF, Apache, LF, OW2, Eclipse)
  - To succeed as a continuing resource, the “commons” must be protected from bad actors (poachers) and replenished over time (repopulation)
- A company’s relationship should be a symbiotic one



RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION’S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Interactive Trivia

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Rights to Software

You find software on the Web that has no license. What can you do with it?

1. Anything you want – it is public domain
2. Nothing – you've been given no permissions

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Rights to Software

You find software on the Web that has no license. What can you do with it?

1. Anything you want – it is public domain
2. Nothing – you've been given no permissions

Software is automatically protected by copyright law!

- The copyright owner's permission is required in order copy, distribute, or modify.
- That permission is expressed in a license.
- You need a license for any software that was not developed by your organization.
- Need to do what the license requires in order to have the permission provided by the license.

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Participating in the Open Source Community

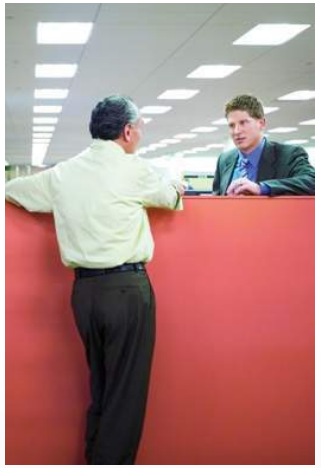
RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

OSS is Different than Commercial Software

To use commercial software in your development process, you must go through ….

Procurement!



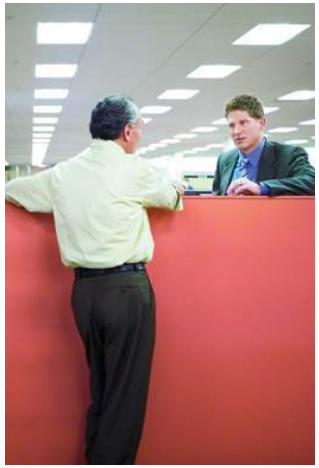
RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

OSS is Different than Commercial Software

To use commercial software in your development process, you must go through ….

Procurement!



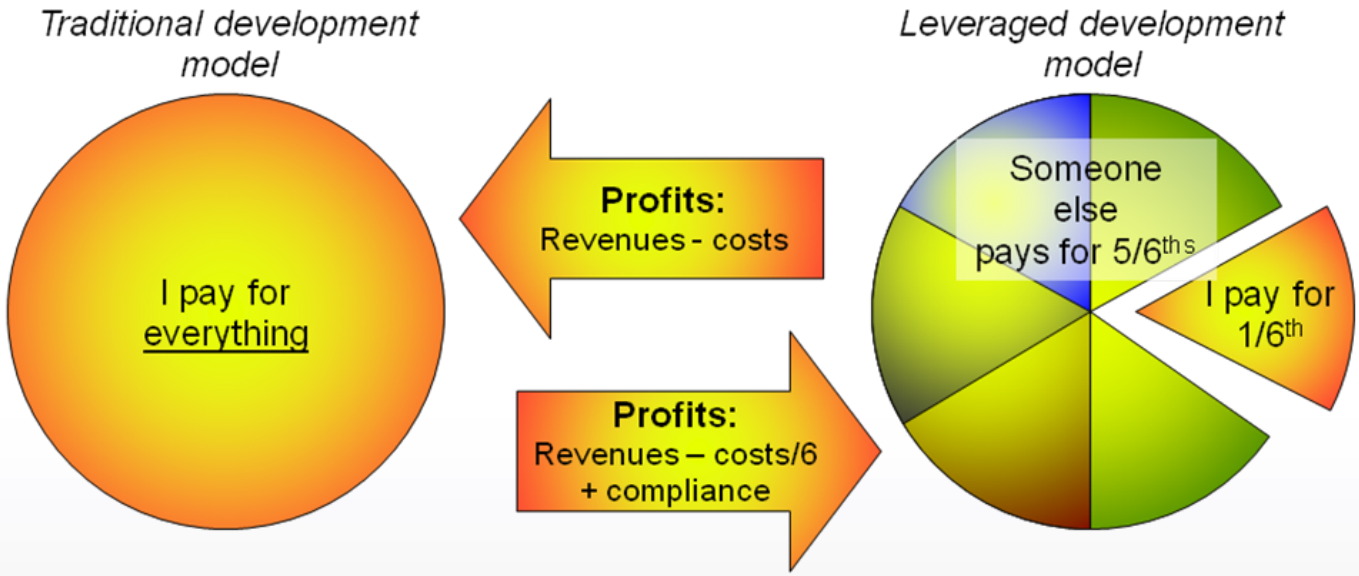
However, OSS pushes procurement to the edges of the organization.

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Why Participate in an Open Source Community?

Leveraged Development

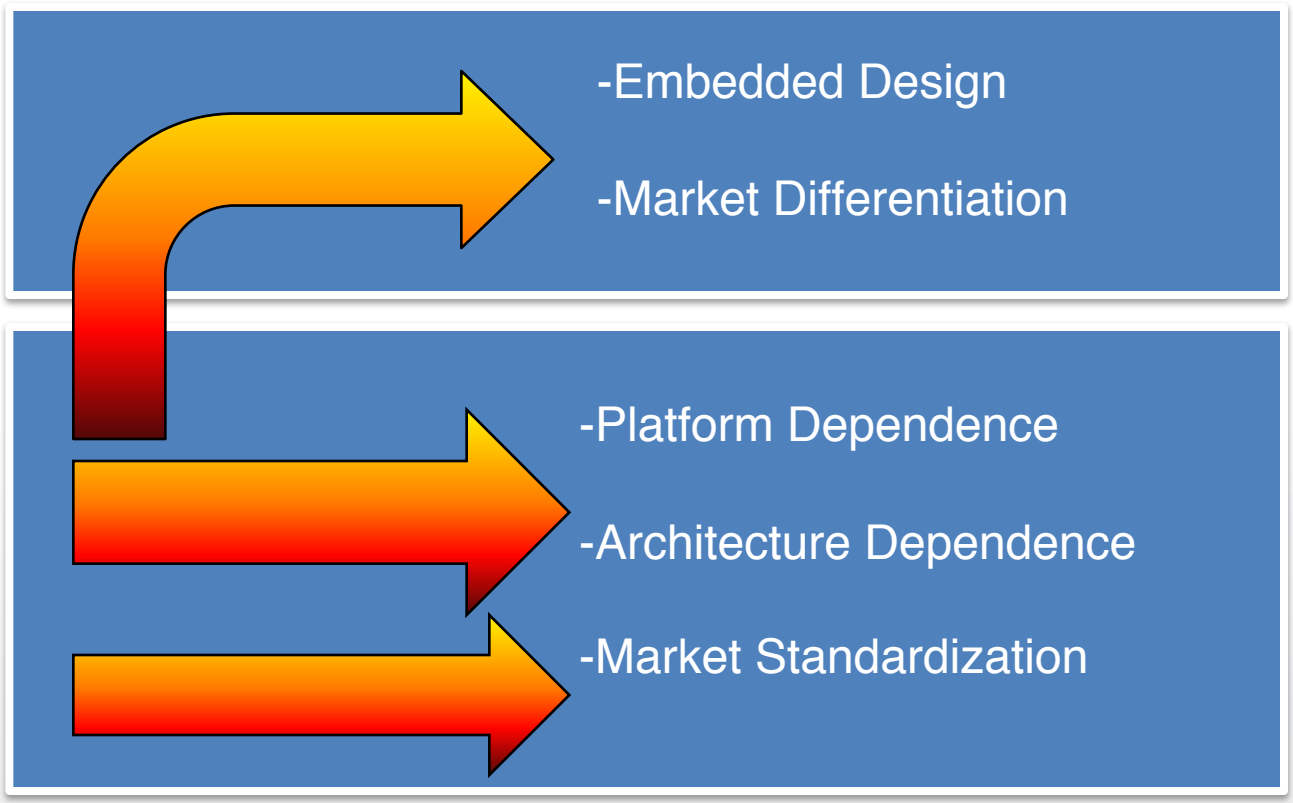


RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Why Participate in an Open Source Community?

Embedded Design and Market Differentiation



RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

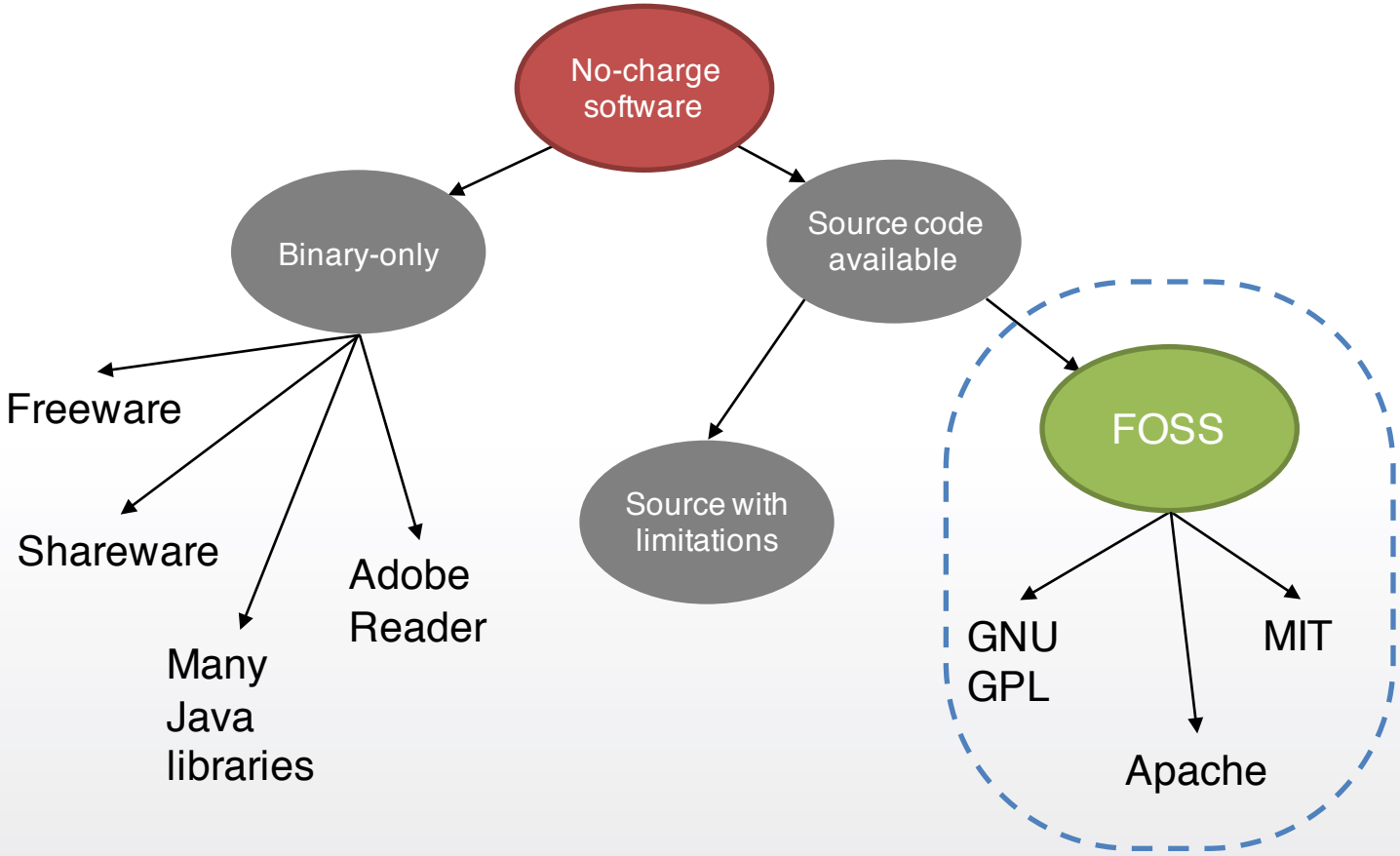
organizational participation in open communities

Licenses in Open Source

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

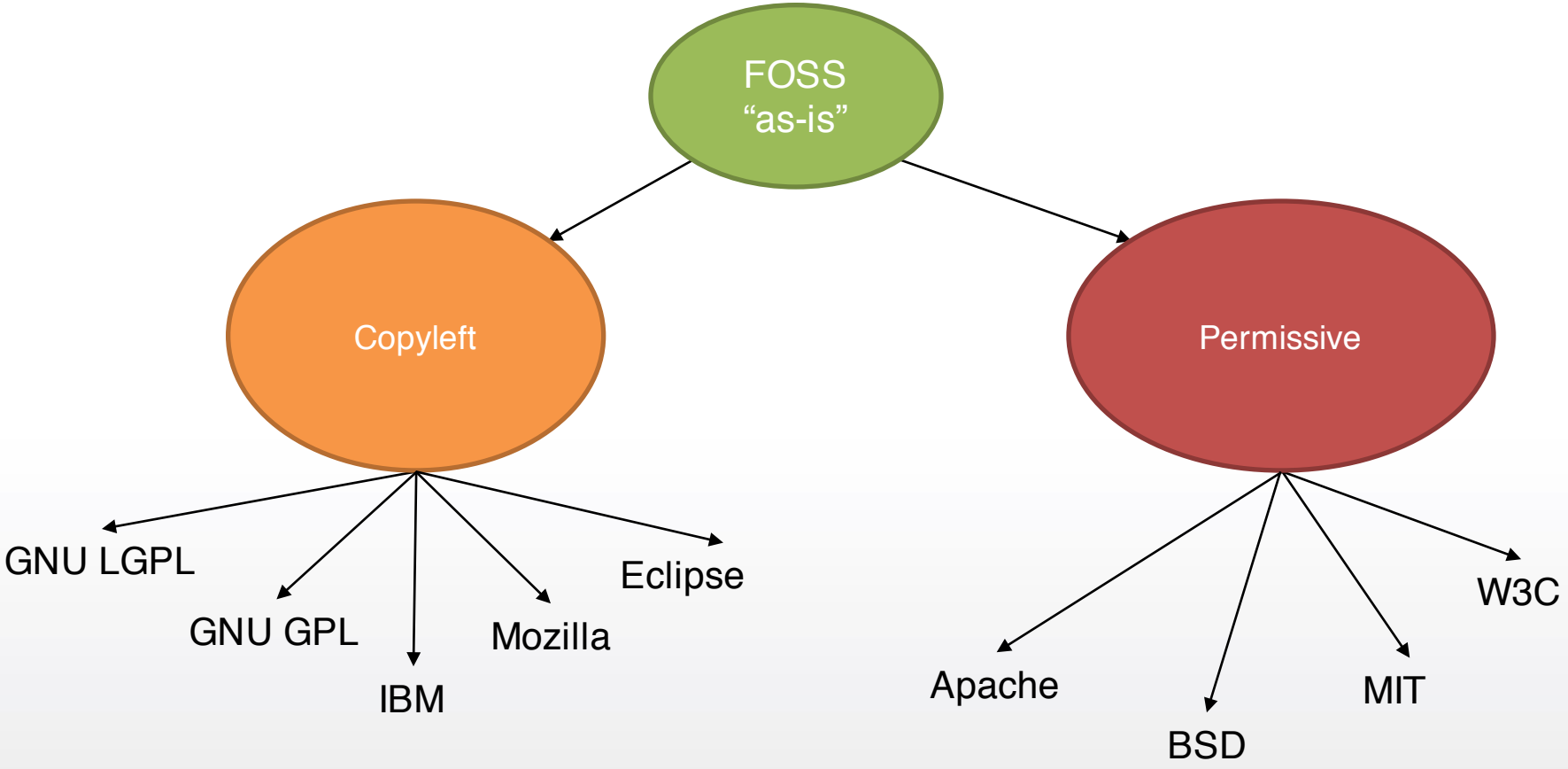
Free and Open Source Software is *Not* the Same as "Free" Software



RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Two Types of FOSS Licenses



RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Interactive Trivia

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Filing a Grievance

How many Linux (kernel or subsystem) developers does it take to file a grievance against an infringer to cause legal action?

a. One – Any Linux maintainer
b. All copyright holders of Linux acting together
c. One – Any copyright holder of Linux
d. One – Linus Torvalds
e. None of the above

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

Filing a Grievance

How many Linux (kernel or subsystem) developers does it take to file a grievance against an infringer to cause legal action?

a. One – Any Linux maintainer
b. All copyright holders of Linux acting together
c. One – Any copyright holder of Linux
d. One – Linus Torvalds
e. None of the above

It only takes one copyright holder to enforce a license

Replace "Linux" with any copyrighted work and the same applies (e.g. BusyBox)

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

CC BY SA

organizational participation in open communities

Open Source Review Policy and Processes

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

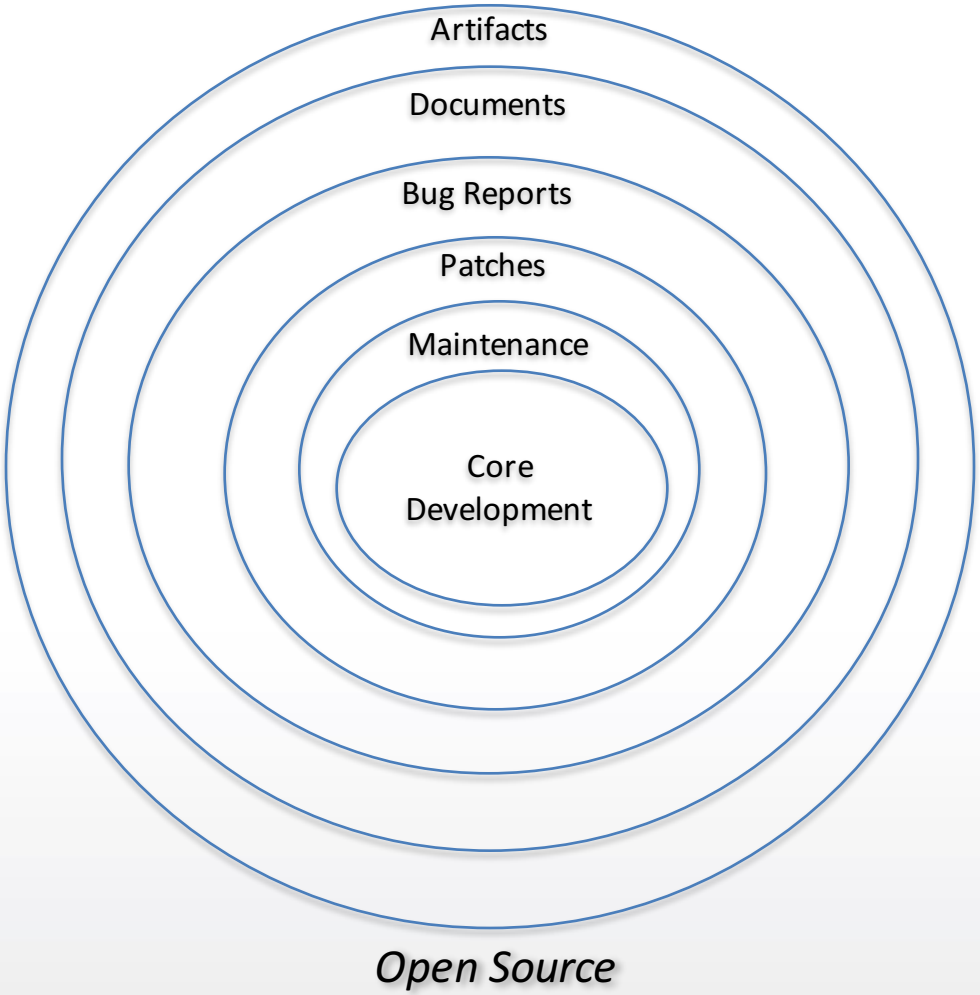
CC BY SA

Sample Open Source Program Office

- Host the Open Source review process
  - Develop Tools/Automation
- Promote/encourage the use of and contribution to Free & Open Source software within the organization
  - Training & consulting with product teams
  - Open Source website
- Promote organization in the community
  - Conference and organization sponsorships
  - External website
- Handle issues associated with organization's use of OSS

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

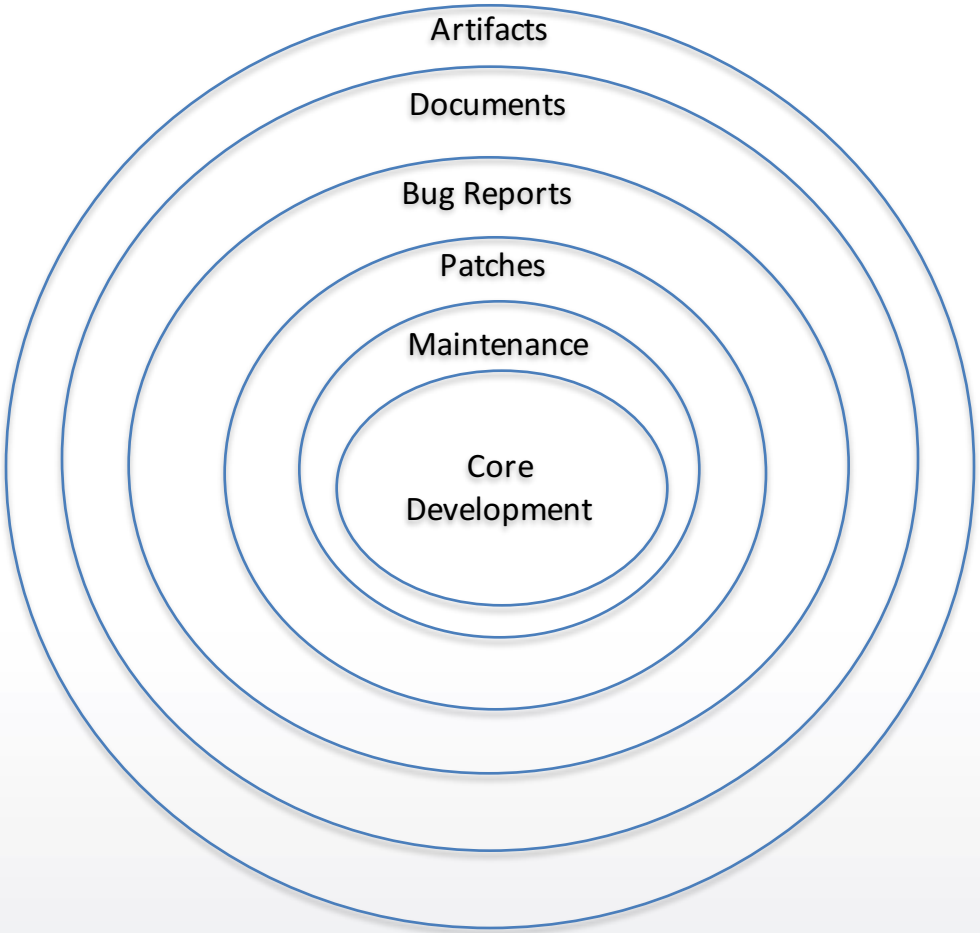
CC BY SA



Open source software is comprised of many layers

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

Nicolas Ducheneaut (2005)

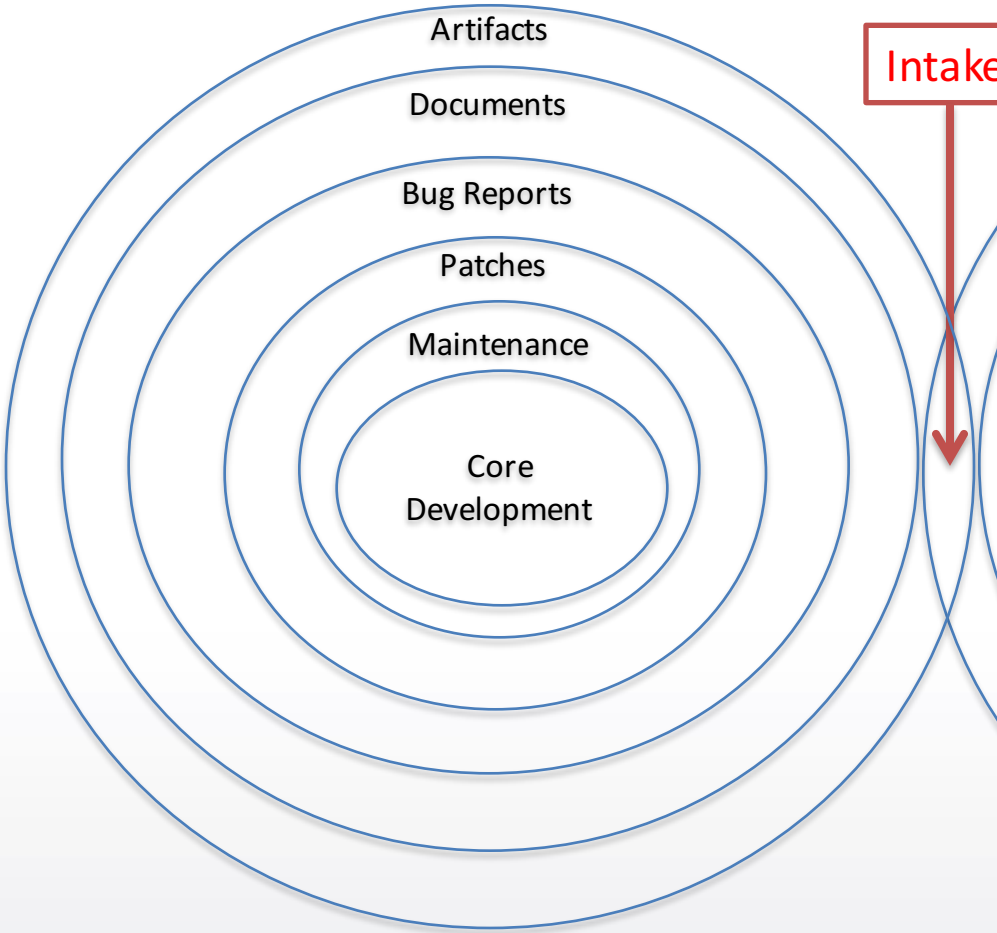


Open Source

Very often, corporations engage open source communities

Corporation

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM



Intake

- Software supply chains
  (e.g. Vendor supplied libraries)
- Developer procurement of OSS
  (e.g. GitHub repositories)

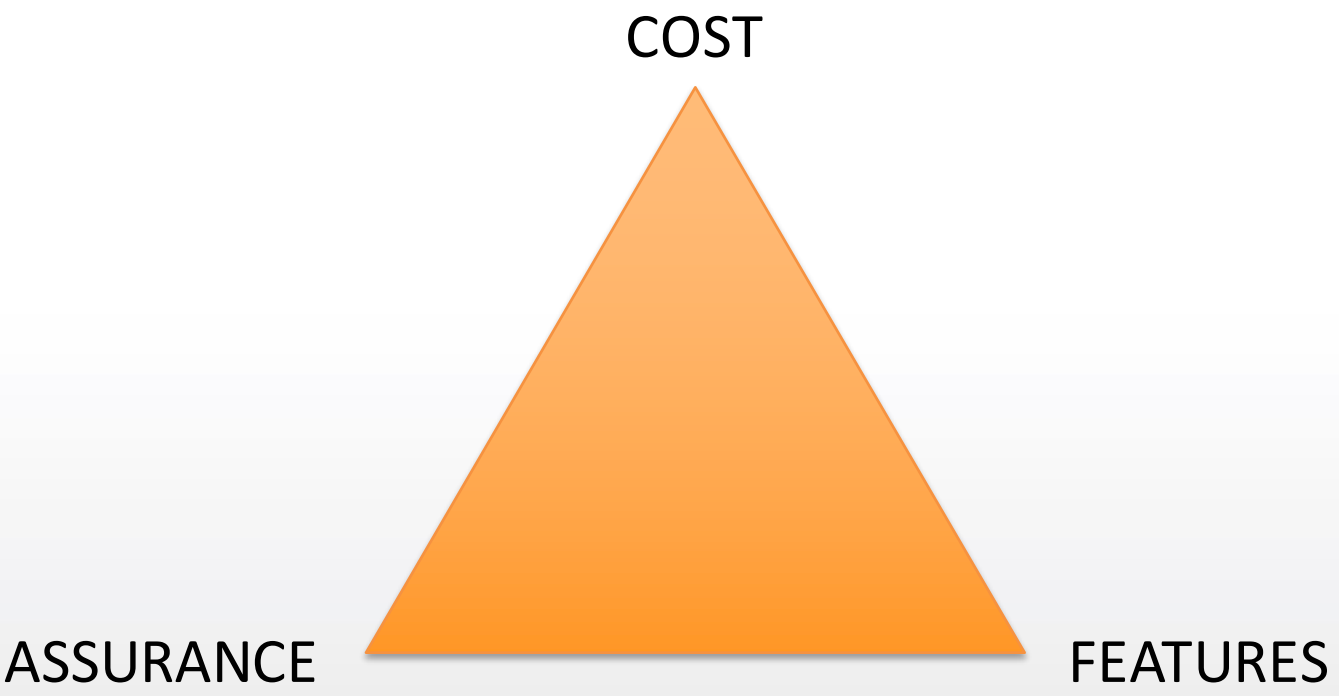
Open Source

Corporation

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

organizational participation in open communities

Balancing OSS Cost, Features and Assurance



RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

The Challenges

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

organizational participation in open communities

The Challenges

- Poorly defined intake can have impact on software deployment
- Poorly defined intake can have impact on internal software relationships
- Poorly defined intake can have impact on internal software vulnerability identification

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

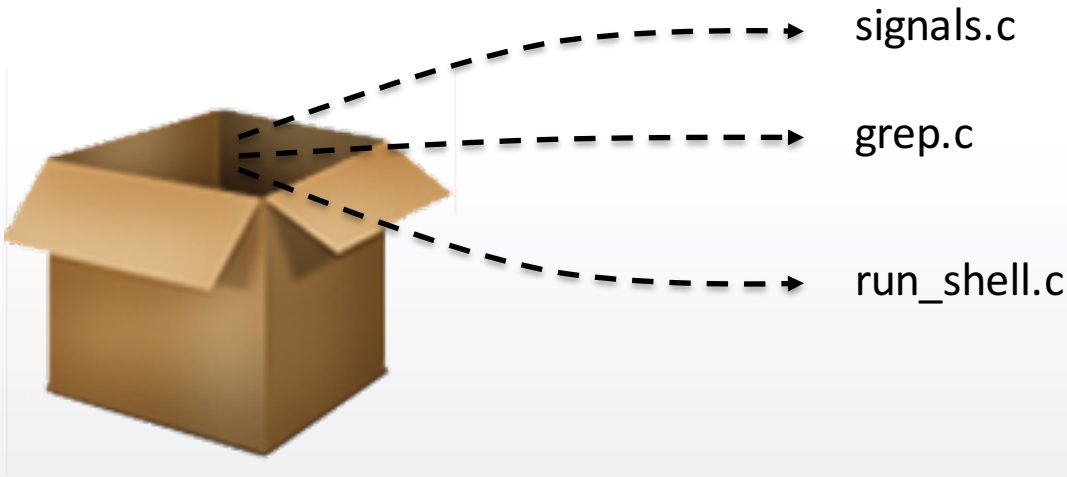
An Example

- BusyBox
  - Unix utilities into a single, small executable

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

An Example

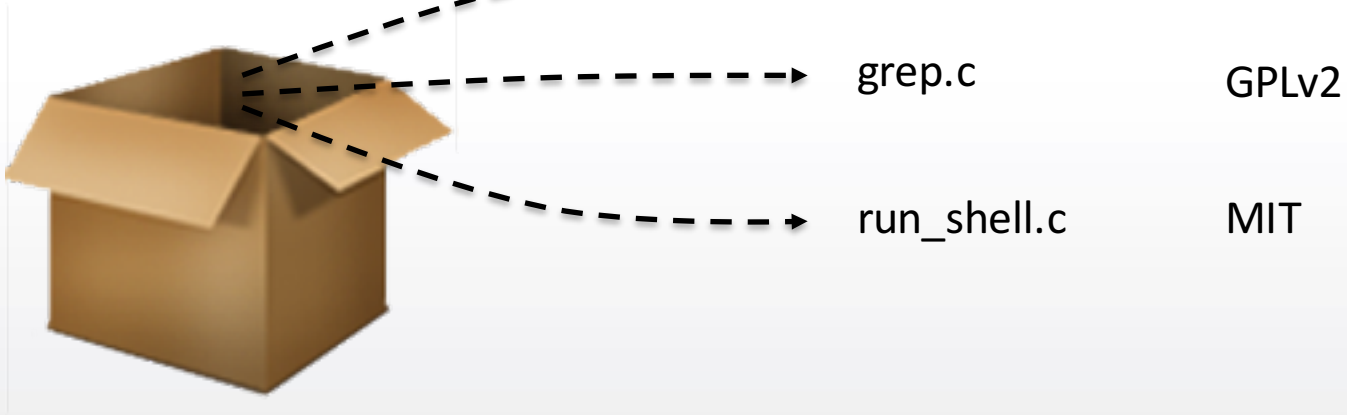
- BusyBox
  - Unix utilities into a single, small executable
  - Comprised of many files



RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

An Example

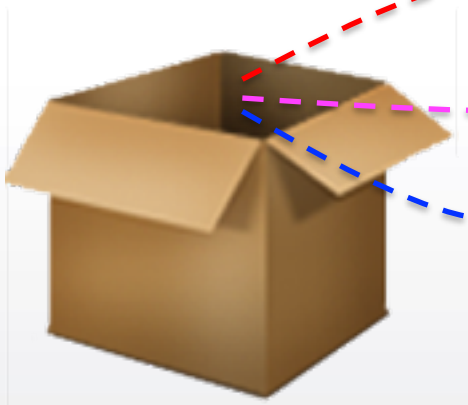
- BusyBox
  - Unix utilities into a single, small executable
  - Comprised of many files



RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

An Example

- BusyBox
  - Unix utilities into a single, small executable
  - Comprised of many files

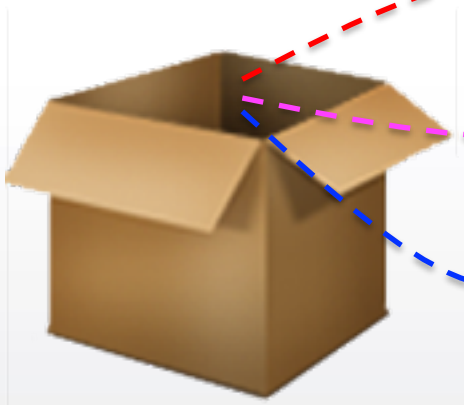


mdev.c	CVSS Severity: **7.2**	Before v 1.21.0	CWE 264
udhcpc	CVSS Severity: **6.8**	Before v 1.20.0	CWE 20
httpd	CVSS Severity: **5.0**	rob_landley:1.01	CWE 22

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

An Example

- BusyBox
  - Unix utilities into a single, small executable
  - Comprised of many files



gcc –Wall: **752 warnings on Debian linux 7.0 64bit**
(sign conversion errors, missing initializer, unused variables, etc.)

cppcheck 1.61: **2 findings on Debian linux 7.0 64bit**
(resource leak and scope reduction possible etc.)

Flawfinder: **3322 findings**
649 findings with high criticality
Use of strcpy (194 times), strcat(77 times), printf without format string

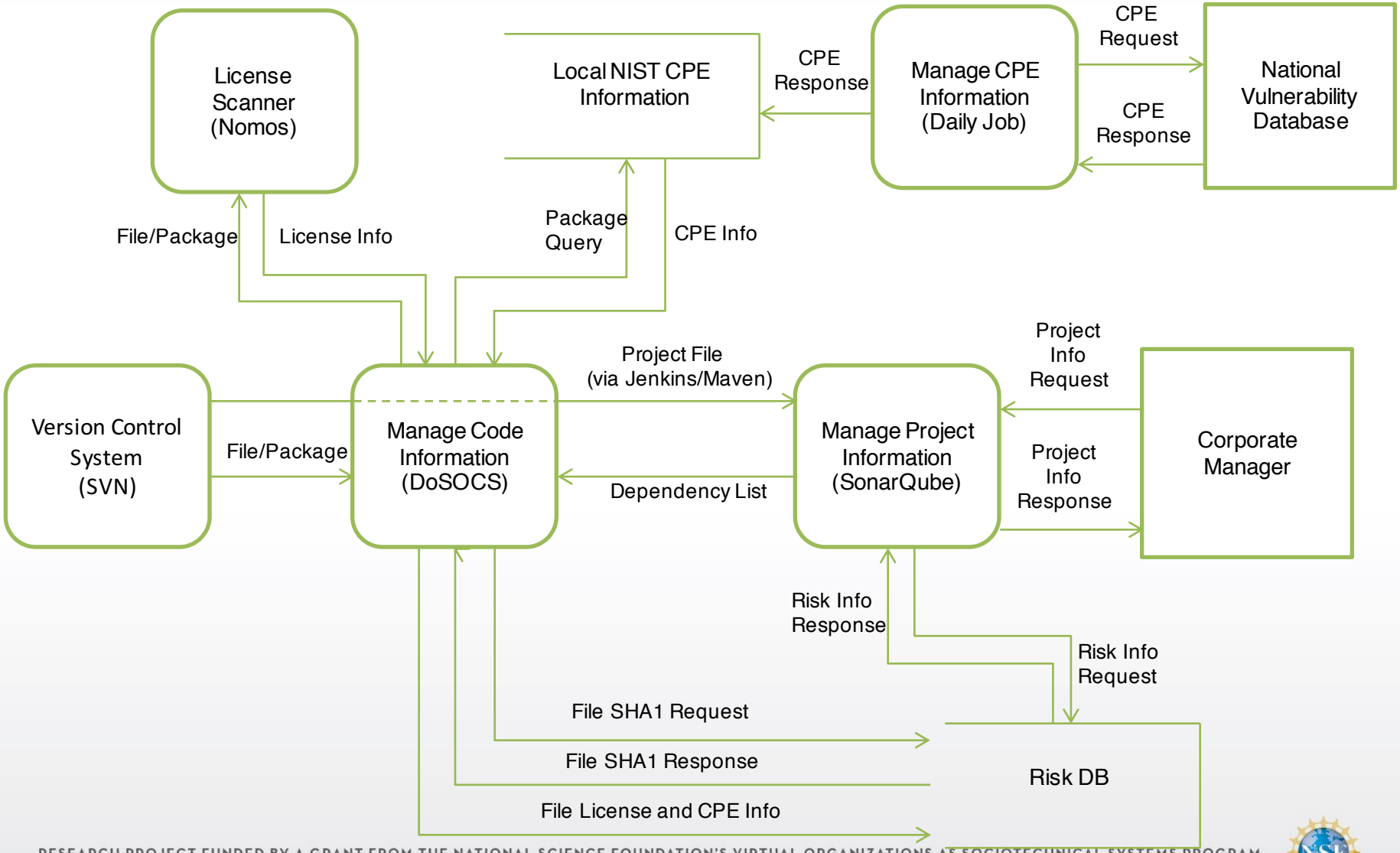
RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

What to do

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

organizational participation in open communities

THIS IS NOT YOUR DFD FOR ASSIGNMENT 1



RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

OSS Maturity Framework

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

organizational participation in open communities

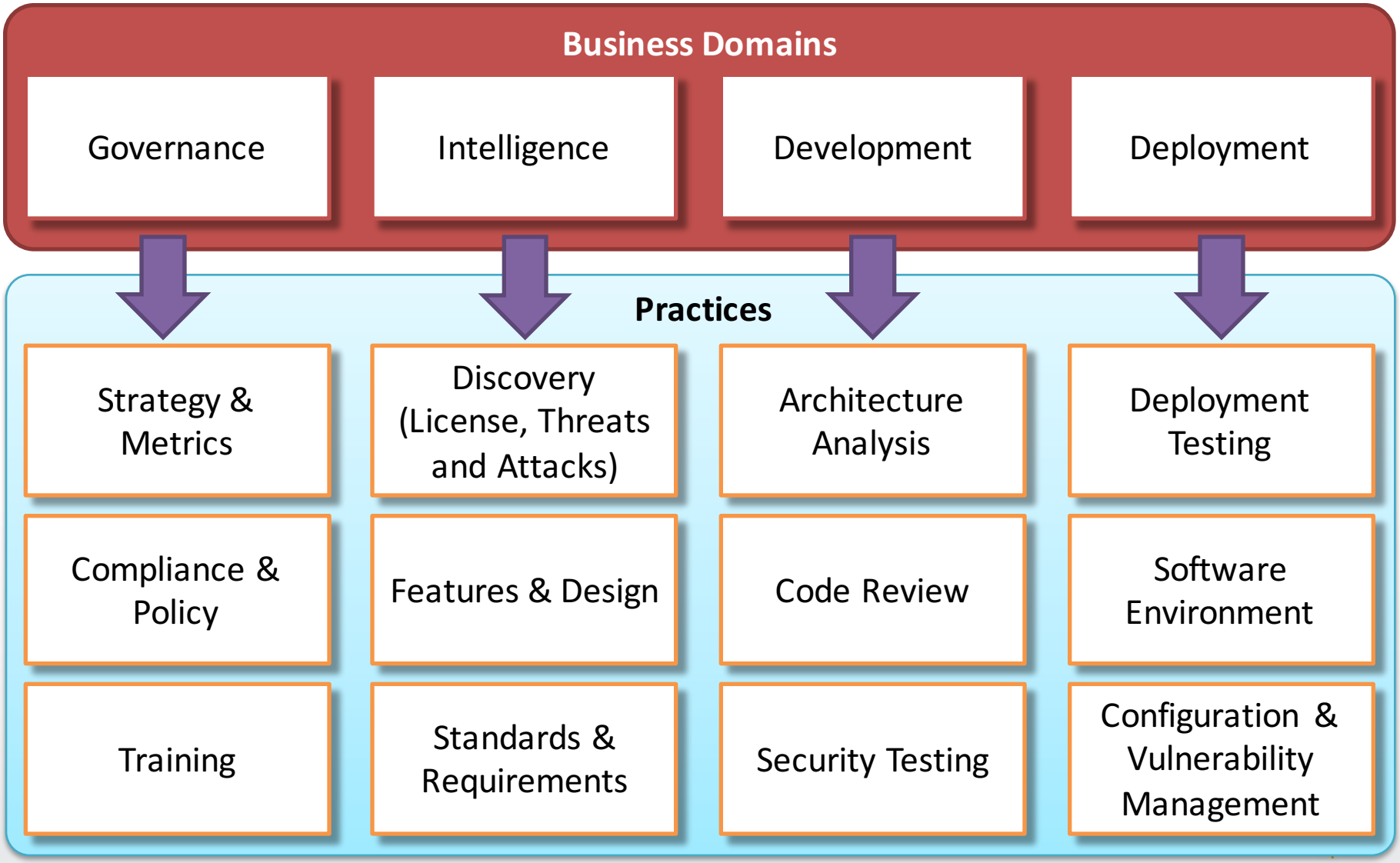
What is an OSS Maturity Framework?

- A measurable framework
- Four business domains organize twelve practices
- Activities under practices in three maturity levels
- Is used to observe, understand, and measure OSS intake

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

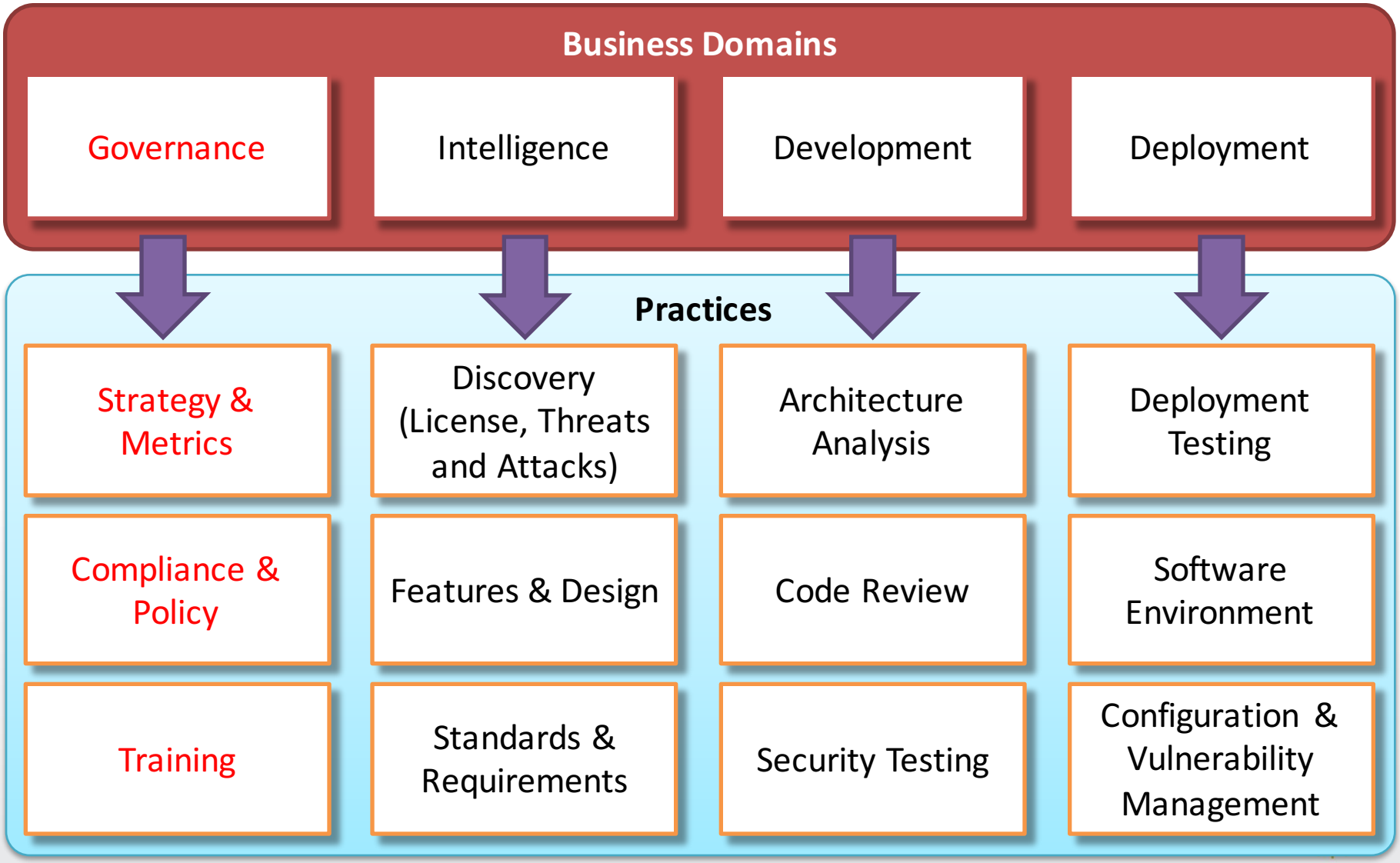
organizational participation in open communities

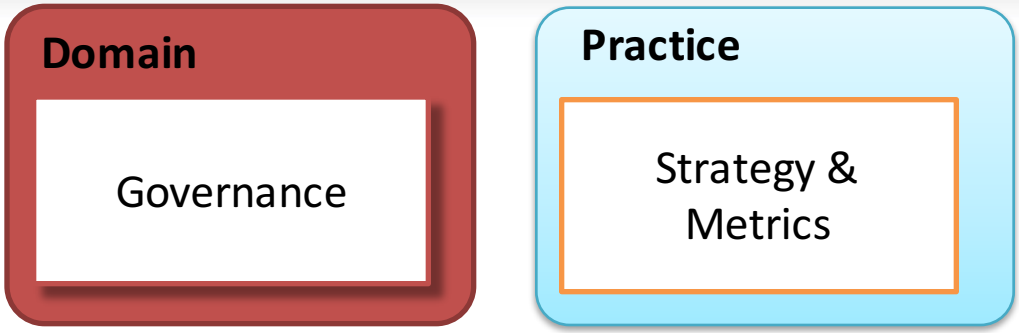
OSS Maturity Framework



organizational participation in open communities

OSS Maturity Framework





Planning, assigning roles and responsibilities, identifying software security goals, determining budgets, and identifying metrics and gates.

Objective	Activity	Level
make the plan to integrate OSS explicit	publish process (roles, responsibilities, plan), evolve as necessary	1
secure executive buy-in before OSS integration	educate executives	
make clear who's taking the risk by integrating a OSS product	require security sign-off	
foster transparency in the OSS intake	publish data about software compliance and security internally	2
change structure to enable OSS intake	enforce gates with measurements and track exceptions	
define success of the OSS product being integrated	identify metrics and use them to decisions	
know where all applications in your inventory stand with respect to the OSS product	use an internal tracking system	3

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

organizational participation in open communities

Domain

Governance

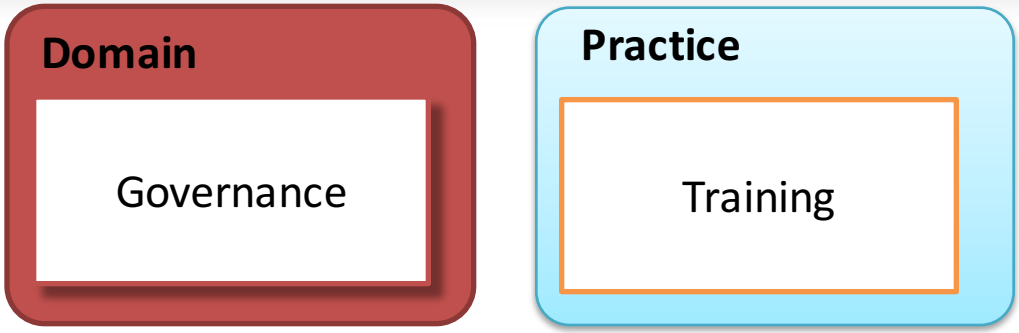
Practice

Compliance & Policy

Identifying controls for compliance regimens, developing contractual controls (COTS SLA), setting organizational policy, and auditing against policy.

Objective	Activity	Level
understand industry compliance drivers (FFIEC, GLBA, OCC, PCI, SOX, HIPAA, SPDX, Open Source Initiative)	building compliance policy based legal context	1
establish guidelines and policies for intake of OSS code	develop written, available, and recorded policies	
align practices with compliance such that OSS integration is compliant with all requirements necessary	implement and track controls for compliance	2
vendors explicate compliance and security when delivering OSS (Vendor is a OSS integrator)	paper all vendor contracts with software security SLAs	
demonstrate compliance story with OSS integration throughout organization (OSS intake as a practice)	create regulator success stories	3
keep policy aligned with reality so that OSS meets compliance requirements with the required metrics	drive feedback back to policy	

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM



Creating programs to educate and train new and existing employees on the policies and procedures related to OSS intake.

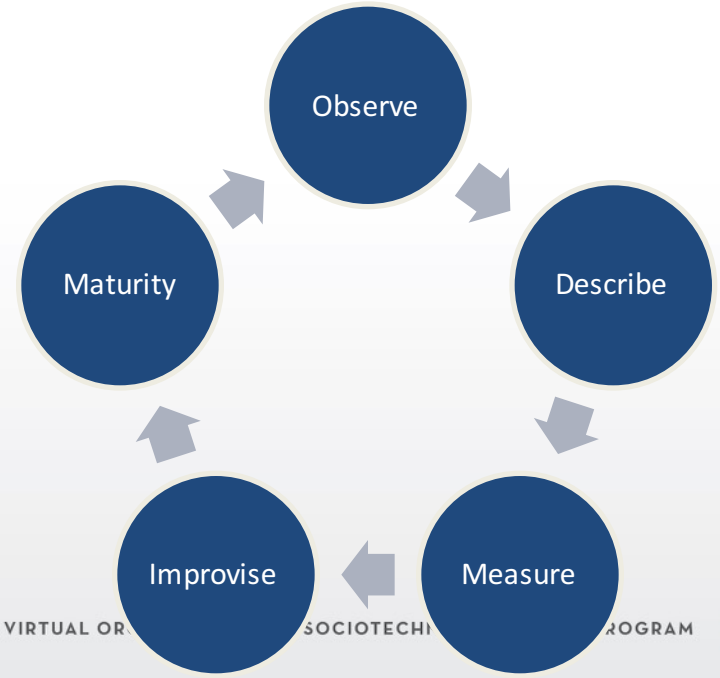
Objective	Activity	Level
promote culture throughout the organization so that OSS integration can be well understood	provide awareness training	1
build capabilities beyond awareness so that developers can under risk associated and seek for guidance	deliver role-specific advanced curriculum (tools, technology stacks, bug tracking)	
ensure new hires enhance culture of the organization to ensure safe OSS integration and right usage over time	include OSS training for new hires	2
create program office resources tied into development so that OSS integration is friendlier experience	identify and distribute on-demand training resources	
spread security culture to providers	provide training for vendors or outsource workers	3
market security culture as differentiator	sponsor external OSS events	
keep staff up-to-date and address turnover	require annual refresher	

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

organizational participation in open communities

Using the OSS Maturity Framework

- Activities are observable
- Scoring each activity helps derive a score
- Activities are organized into 3 maturity levels
- Score can be obtained for
  - Practice
  - Domain



RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL OR SOCIOTECHI ROGRAM

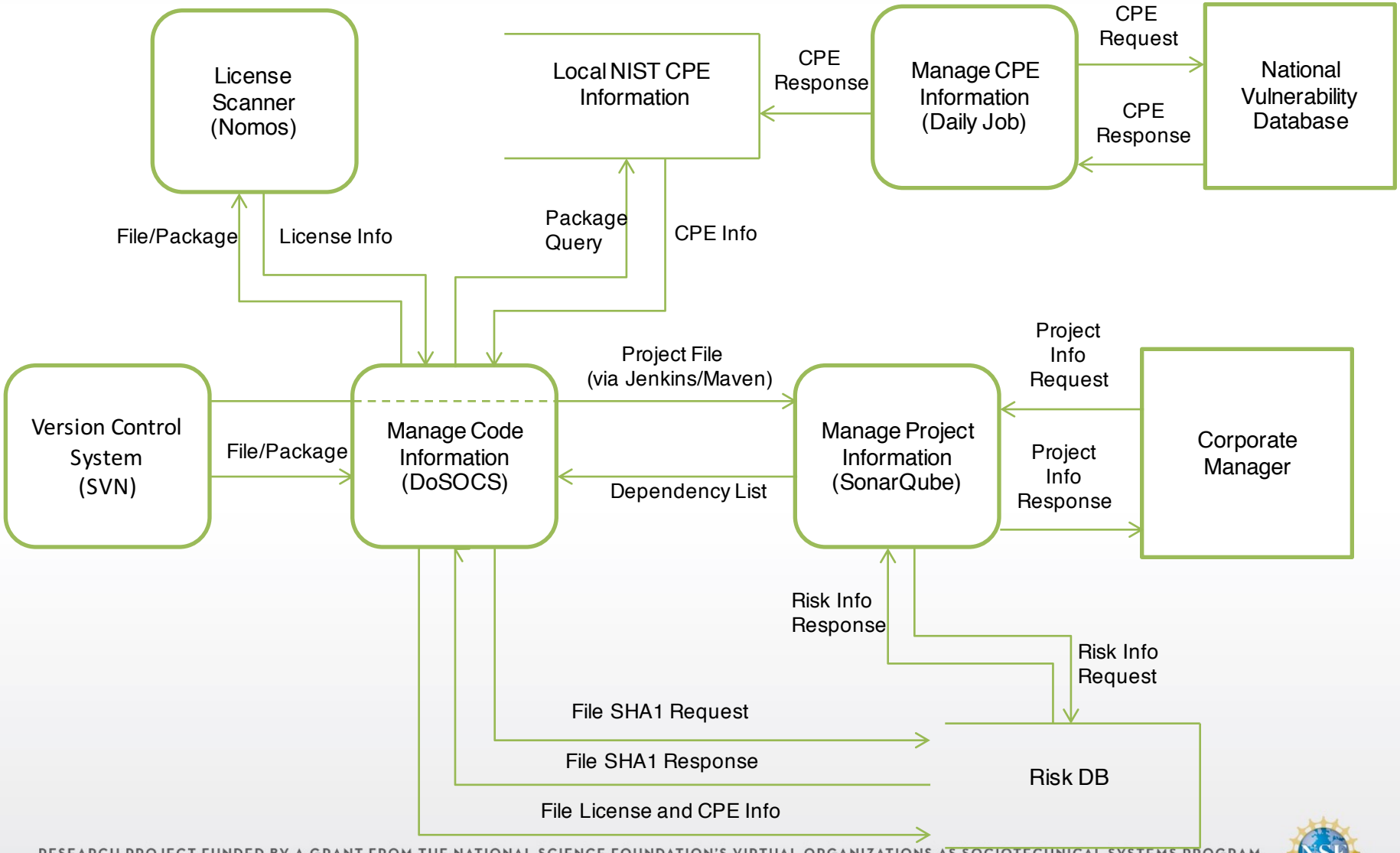
Key Objectives

- Understand existing OSS practices in an organization
- Find cost and benefit balance of new OSS practices
- Create clearer OSS picture from which to advance future OSS strategy through established maturity model

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

organizational participation in open communities

THIS IS NOT YOUR DFD FOR ASSIGNMENT 1



RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

The Future of Open Source 2016

- 47% of all companies don't have formal processes in place to track OS
  - 50% of companies who have policies don't enforce them or can be bypassed
- 65% of surveyed companies use open source
  - Up from 60% in 2015
- 76% of respondents have plans to use containers
  - 36% for testing
  - 37% for development
- 66% of respondents don't have a person dedicated to OS resource mgmt.
  - In over 50% of companies, there is no one responsible for vulnerability remediation

- https://www.blackducksoftware.com/2016-future-of-open-source

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM

HAVE A GREAT WEEKEND!!

Assignment 1 Due Monday!!

RESEARCH PROJECT FUNDED BY A GRANT FROM THE NATIONAL SCIENCE FOUNDATION'S VIRTUAL ORGANIZATIONS AS SOCIOTECHNICAL SYSTEMS PROGRAM