BRITISH COLUMBIA
The Best Place on Earth

Ministry of
Citizens' Services

Guidelines on the Use of Open Source Software

Release 1.0 April 2012

Architecture, Standards and Planning Branch

Office of the CIO · Province of BC

People · Collaboration · Innovation

Guidelines on the Use of Open Source Software

This document is prepared by the Office of the Chief Information Officer (OCIO) for the Province of British Columbia. It provides a Provincial perspective on the use of open source software. It discusses the business benefits and risks that are associated with the use of open source software and provides principles and guidance for adopting open source software by the Province of British Columbia.

This document addresses the use of open source software. The modification and re-publication of open source software by the Province of British Columbia leads into topic areas not addressed in this document.

Introduction

The purpose of this document is to introduce its readers to the topic of open source software and to offer some guidance for the use of open source software by or on behalf of the Province of British Columbia.

The term "open source software" or OSS refers to software applications that are made available in source code form under a license agreement that imposes very few restrictions on the use, modification and redistribution of the source code. Open source software is commonly made available at no cost.

The OCIO position on open source software is neutral: there is no overarching preference for commercial software or for open source software. The choice of a software solution should be based on the business value proposition, the total cost of ownership and an assessment of the associated risks.

Open source software development began as a small cottage industry. Over the past 30 years the open source movement has steadily grown and evolved. Today open source is a recognized strategy that organizations may choose to meet their needs and pursue their goals.
This document offers guidance on things to consider when open source software is being proposed or evaluated for use by the Province of British Columbia.

How is Open Source Different from Proprietary Software?

Traditional proprietary software involves a variety of restrictions imposed through a license agreement. The aims of these restrictions are to protect the property rights of the author.
The open source software community takes an approach that emphasizes the rights of the user.

Open source software is licensed to users with the following freedoms:

- The software may be used for any purpose.
- The source code may be studied and modified.
- The software may be redistributed without royalty payments or other restrictions.

It is these kinds of freedoms that are foundational to open source software. They provide the transparency needed for community peer review, which improves quality and robustness.

Secondly, open source is developed primarily by volunteers. Although in recent years development is increasingly done by "paid volunteers" from the private sector. Development is hosted on the Internet, which means that volunteers can collaborate from anywhere on the planet. The volunteers themselves vary in ability from hobbyists and amateurs to dedicated professionals and subject matter experts. Their motives range from communitarianism to enlightened self-interest.

Thirdly, the development process itself is highly transparent. When issues emerge about the viability or direction of a project they are usually highly visible. This is good, because not all open source software projects are robust. And no one wants to deploy a system only to discover later that the system has a doubtful future.

Why is a Clear Definition for Open Source Software Important?

In the marketplace, software is distributed under many types of licenses: shared source, community source, shareware, freeware and others. The proliferation of license types leads to misunderstandings and incorrect assumptions about open source software. This situation is further compounded by the difficulty the average person has understanding license agreements.

There is an easy way to simplify this problem. The Open Source Initiative (OSI) is an organization established to promote open source software. The OSI publishes an Open source definition that is widely accepted. Furthermore the OSI has a process for reviewing and approving licenses. They publish a list of licenses (currently around 70) that conform to the OSI definition.

> *The OCIO recommends that the Province use the term "open source software" to refer exclusively to "software that is distributed under a license that is endorsed by the Open Source Initiative (OSI)".*

In practice, 9 of the 70 OSI endorsed licenses are the most widely used ones. Thus, adhering to a standardized definition of "open source software" should help streamline the procurement process by limiting the amount of intervention needed to ensure the Province's rights and obligations are understood and acceptable.

What Advantage is Open Source Software from an Organizational Perspective?

Less process. Open source software rarely involves an up-front purchase cost. Therefore, acquiring open source software can involve fewer approvals, fewer meetings, less process and delay resulting from the financial approvals process inside government. When facing deadlines less process is a welcome.

Greater flexibility. Licensing open source software does not involve negotiating a contractual agreement for the software. No contract means less commitment, which in turn means the Province has more flexibility if plans need to change.

Better sustainability. Market forces can undermine the sustainability of a software product. A software system can become redundant through the consolidation of an overcrowded market or through strategic mergers and acquisitions. Adopting an open source solution is a strategy to help insulate I/T investments from external market forces. Having "open source" rights to the application code reduces dependencies.

Greater freedom. In the open source model of development third party vendors compete to offer software support. Having "open source" rights to the application code ensures vendor lock-in is not a concern.

Self determination. Open source systems are developed in an open, collaborative manner. Supporters can exert an influence on a system's direction. Users have direct input into improvements and setting priorities.

What are Some Potential Legal Issues of Using Open Source Software?

In simply acquiring and deploying open source software, an area of concern is the potential consequences of unwittingly infringing the intellectual property (IP) rights of someone. This can happen when software includes code of disputed ownership. IP infringement can result in disruption and/or have negative financial consequences to the end user.

The uncertain possibility of IP infringement via open source software is best dealt with through risk management. Evaluate the risk. How likely is the risk? What are the consequences? Is the risk acceptable or should it be mitigated? What options are available to mitigate such risk? What steps would a reasonable person take?

Some open source software is marketed with user indemnification bundled into the product. Third party insurance is also available that indemnifies users of designated open source software. Services are also available that review and rank open source software in accordance

with its various aspects of interest to prospective users (i.e., a kind of Consumer Reports approach.). For further advice on managing risks you may wish to consult the Province's Risk Management Branch.

Another consideration is the Provinces existing legal/contractual arrangements. Not all software licenses can be assumed to be mutually compatible[1]. Core policy requires a legal review of the contract terms for new software licenses, both open source and proprietary.

More information and assistance may be available through the Province's Legal Services Branch.

What are the Operational Issues of Open Source Software?

Under the open source software development model the source code is open to public scrutiny and peer review. Thus any coding vulnerabilities in a system can be spotted and quickly fixed. Unfortunately this also means vulnerabilities can be spotted and quickly exploited too. It is common practice that attacks are developed that target known vulnerabilities on unpatched systems.

It is important that software, open source or proprietary, be maintained in a timely, systematic manner. Security advisories should be monitored and reviewed regularly. Patches should be applied soon as they become available. Updates should be applied as soon as practicable. Systems of concern (i.e. for which the risks are greater) should maintain a "system security plan"[2]. The responsibility lies with the business program area to ensure that risks are being assessed and business application software is being properly maintained.

Business continuity is another important consideration. Critical business functions need to be available to users and customers on demand. When selecting software a business area should ask itself questions about the impact of open source on business continuity. There are many aspects to consider. How long has the project existed? Is the project healthy, well organised? Does it have a corporate sponsor? Is the software mature or underdeveloped? Are software updates published on a regular basis? Does the project publish a technology roadmap? Is the

1 Commonly heard is that the Province's Oracle license prohibits the use of Oracle products in combination with any software released under the GNU license. The Province's primary Oracle license contains no such prohibition.
2 SANS offers the following explanation: The purpose of the system security plan (SSP) is to provide an overview of the security requirements of the system and describe the controls in place or planned, responsibilities and expected behaviour of all individuals who access the system.

software in wide use? Is there a stable community of users? Have they voiced issues with the project?

The impact of open source on business continuity should be understood and managed accordingly. Consider some questions like: "what would we do if... ". Managing risk means having a mitigation plan. Once fully understood a risk may be worth taking, or not. Either way the decision should be informed by facts. This approach is much less stressful than depending on opinions.

Help with risk management is available through the Province's Risk Management Branch and the Information Security Branch. Third party services are available that rank open source software in accordance with its various aspects of interest/concern to prospective users.

Open source software may be acquired for free, but maintaining any software in a production environment costs money. Factor the ongoing costs into the cost of the decision.

Principles for Adopting Open Source Software

1. The OCIO recommends that open source licensed software be defined as "any software that is distributed under a license endorsed by the Open Source Initiative".
2. Open Source Software must be given impartial consideration (alongside proprietary software) when being proposed in response to a procurement.
3. The choice of software should be based on the business value proposition, the assessment of the associated risks and compliance with standards.
4. Acquirers must ensure their intended use of open source software is compatible with the software's license terms.
5. Acquirers must ensure that the sources used for downloading and updating open source software are trustworthy.
6. Acquirers must undertake to keep their open source software patched and up-to-date, consistent with best security practice.

Further Guidance

- The OCIO endorsement of OSI approved licenses is not an endorsement for the use of any proposed software.

- The use of open source software (and proprietary software) must meet the Province's requirements for privacy and security.
- All software selections should be suitable for integration with existing infrastructure investments, such as identity management.
- Software distributed under licensing agreements known as "freeware", "shareware", "community source" or "shared source" (i.e. not OSI approved) are not endorsed by the Province unless authorized by the OCIO on a case by case basis.
- The acquirer must ensure that contracted providers of software notify the Province of any open source software components used in a deliverable.
- Core Policy Chapter 6 requires that all information technology procurement be done through Shared Services BC[3].
- Acquirers must follow the STRA standard to evaluate the risks of software plans by using the Province's Information Security Management and Risk Tool (iSMART).
- The Province's Legal Services Branch and Risk Management Branch may be able to provide additional assistance.

Glossary

Acquirer – an employee, contracted resource, program area or business unit that acquires software for or on behalf of the Province of British Columbia.

Total Cost of Ownership - is a financial estimate whose purpose is to help consumers and enterprise managers determine direct and indirect costs of a product or system.

3 Chapter 6 of CPPM applies when downloading and running of opens source software on behalf of the Province.

References

Open Source Definition:
http://www.opensource.org/osd.html
OSI Approved Licenses:
http://www.opensource.org/licenses/alphabetical
Example of Vendor Indemnification:
http://www.oracle.com/us/technologies/linux/ubl-indemnify-066152.pdf
Example of Third Party Indemnification coverage:
http://www.openlogic.com/products/indemnification.php
Ministry of Finance, Risk Management Branch:
http://www.fin.gov.bc.ca/PT/rmb/index.shtml
Ministry of Labour, Citizen's Services and Open Government: Information Security Branch
http://www.cio.gov.bc.ca/cio/informationsecurity/index.page
Questions about this document? Please e-mail ASB.CIO@gov.bc.ca