

The AuditNet® Monograph Series

“Is Your IP Leaking?”



Rob Harmer

<http://www.pcprofile.com>

Copyright © 2004 Rob Harmer Consulting Services Pty Ltd

AuditNet®

Preface

The Monograph series grew out of a desire by Jim Kaplan to establish an online electronic communication network for auditors. Before online services, bulletin boards and the Internet many auditors were operating without the benefits of peer collaboration and information sharing on a major scale. The Internet, founded on the principle of sharing and communication, changed the interaction model between auditors. Auditors can now post messages in online discussion forums, upload and download audit work programs, checklists, surveys, questionnaires and other audit related material in warp speed. Small one-person audit shops can now communicate with others and feel like they are not paddling upstream with one oar when it comes to having access to audit resources. My vision of an online information communication network for auditors has become a reality with AuditNet® as the foundation.

The AuditNet® Monograph Series or AMS provides auditors with guidance on different aspects of the audit process and other relevant topics to help them do their jobs. New auditors will seek these guides to learn some of the basics of auditing while experienced auditors will use them as a review. Each guide focuses on a specific subject.

This monograph was written exclusively for AUDITNET.ORG by: PCProfile and published in May 2004 by Rob Harmer Consulting Services Pty Ltd P.O. Box 196 Modbury North Sth Australia 5092 phone +61 (0) 418 817 955 fax +61 8 8265 1961

*PC Profile is Australia's ONLY anti-piracy (self-help / non-policing) advisory service and solutions provider based in Adelaide, Sth Australia email: rharmer@internode.on.net
<http://www.pcprofile.com>*

This article and contents is Copyright © 2004 Rob Harmer Consulting Services Pty Ltd

If you have an idea for additions to the AMS please send a proposal via email to editor@auditnet.org

TABLE OF CONTENTS

Preface 2
Overview 4
 Why bother? 4
Now, do we have your attention? 4
Software Licensing 101 4
Open Source has licenses too! 5
Open Source “Contributions” 5
Grant Of Rights – ie; what you are GIVING AWAY! 6
The Problem..... 6
An Often Too Common, Scenario 6
But, we have a legal agreement! 8
How many Open Source Sites? 8
What needs to be considered? 9
A Helicopter View 10

Overview

If you are an auditor one of the tasks you need to do from time to time is audit and validate the list of Intellectual Property (IP) held by your organization.

Never done this before?

Then add it to your lists of tasks to do as the issue faced in one specific area regarding Open Source software might alert you to some risks you not have known until now even existed!

Why bother?

It should already be a well known fact that Intellectual property can be the key differentiator that discriminates your organization, your business, your products, your technology and processes from the opposition and competition. If you don't know this, then you don't understand your business!

However, if you do understand and believe this to be true for your business, then you need to vigorously record all IP developed "within your walls" irrespective of whether it is done by employees or contractors, consultants or 3rd parties, and this includes a check from time to time through an audit work program, that your IP is being adequately protected, at all times.

Many organizations employ specialist IP managers and Legal Counsel to track, manage and vigorously defend the organizations IP. This is a long term position that needs to be understood at the very top of the Executive Tree and should not be taken as a short term view "quick fix" approach as the risks and the rewards can be high if the IP leaks away to other parties!

We suspect that many IP specialists may have missed the point, or not be aware of, the Open Source software issues that we raise here in respect of IP protection in this Monograph

Now, do we have your attention?

You need to stay alert to some unseen threats that may have escaped your notice up until now.

This AUDITNET monograph focuses on the issues all auditors face with OPEN SOURCE software licenses being deployed in organizations, and the resultant intellectual property rights inherent and developed.

- You don't know what we mean by "Open Source"?
- You didn't know there was a "problem"?
- What do we mean by "Your IP is leaking?"?

This Monograph will alert all auditors and IP specialists about what to watch out for as there are some tricks and traps that may be being used by computer staff sometimes unknowingly due to ignorance that might cause some grief for your organization, as your IP leaks out the front and back door!

Failure to start looking into the specific issues that you face within your organization with Intellectual Property, MAY NOT leave you as well protected as you should be. The sooner you start the discovery process, the sooner you can institute policies and procedures and audit work programs to make sure you are protected!

Software Licensing 101

All software is covered by "a license to use" which details the terms of conditions of use of the software and is a general format that has been evolving over a number of years. This article does not discuss the full ramifications of software end user license agreements (EULAs), we will leave that for another Monograph!

Open Source has licenses too!

Open Source software came upon the scene many years ago with a consensus view in the technical user community (software developers, researchers and the like) that all software classed as Open Source would in fact be OPEN and FREE TO USE according to a GNU license with the major distinction being that use of the source code WAS PERMITTED, with some conditions.

NOTE: Under a EULA for commercial-off-the-shelf shrink-wrapped software, use of the source code was not permitted as one of the key conditions contained in commercial EULAs is the requirement to PREVENT reverse engineering or derivative works. These are covered under Copyright provisions of the various jurisdictions where the license is issued.

For a full definition of Open Source see <http://www.opensource.org/docs/definition.php> and for an example of an Open Source Software License see <http://opensource.org/licenses/osl-2.1.php>

An example embedded in some FREE source code, with some atypical conditions is shown here;.

```
# This program is free software; you can redistribute it and/or modify it under
# the terms of the GNU General Public License as published by the Free Software
# Foundation at: http://www.gnu.org/copyleft/gpl.html
```

On the face, using Open Source software seems a great way to go for organizations who need access to free software and source code so as to minimize software ownership and licensing requirements within their organization. The upsurge in Linux within the user and business community owes, in part, some of its success to the free software promoters who have been (for ages) against the megapoly conditions conducted by Microsoft, et al when it comes to software licensing. Many government agencies and business are moving across to Open Source solutions for this reason as they see a cheaper Total Cost Of Ownership (TCO) although the jury is still out as many \$ factors are hidden when looking at both sets of equations, again this is not for discussion here.

Open Source “Contributions”

Common Public Licenses such as listed at <http://opensource.org/licenses/cpl1.0.php> require that any derivative works that are made from an “Open Source” software application must have a “contribution” which constitutes the derivative code and alterations made, made freely available back into the public domain with a “Grant Of Rights” for all to use!

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

Grant Of Rights – ie; what you are GIVING AWAY!

Now read the fine print folks.

This is where your “Open Source Contributions” take on a whole new dimension and are made tricky **and more difficult to manage** when it comes to matters of Intellectual Property! Details here are extracted from <http://opensource.org/licenses/cpl1.0.php>

2. Grant Of Rights

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

The Problem

The key issue you have to face - is how will you know what has been “contributed” from your Open Source source code has been done in a manner that is legally in synch with your company or organizational policies on Intellectual property?

Do your IP staff (you do have an IP register don't you?) keep a physical / electronic register of all IP created and they are making sure they don't violate your policies on handling and managing Intellectual Property?

An Often Too Common, Scenario

A new person joins the organization, (maybe several joining at once) due to an expansion/growth program and they come straight from University/College as graduates with specific skills in Open Source software. After all the position you advertised called for skills in Open Source and they had to demonstrate their knowledge etc at interview time as they were grilled on their suitability!

As a condition of employment staff and contractors are generally obligated to sign their terms and conditions of employment “as is” (that may already include some “standard” [NOTE: These really are very loose and not very tight for control of IP] clauses on IP) such as;

3. It is agreed that at the end of this contract, the incumbent will not take or keep any document, report, project, data, product, etc., resulting from this agreement without permission from the supervisor and the company.
4. The incumbent solemnly declares that he/she will not divulge without prior authorization, any information or data that he/she obtains as a result of this employment.
5. Products produced by the incumbent as a result of this agreement and during the term of this agreement belong jointly to the supervisor and the company, unless otherwise agreed between these parties.

or

3.8 Ownership of Intellectual Property

Any and all intellectual property, including but not limited to copyright, invention, trademark, trade name, service mark, and/or trade secrets created or conceived pursuant to or as a result of this contract and any related subcontract ("Intellectual Property"), shall be work made for hire and the State shall be considered the creator of such Intellectual Property. The agency, department, division, board or commission of the State of xyz requesting the issuance of the contract shall own (for and on behalf of the State) the entire right, title and interest to the Intellectual Property throughout the world. Contractor shall notify the State, within thirty (30) days, of the creation of any Intellectual Property by it or its subcontractor(s). Contractor, on behalf of itself and any subcontractor (s), agrees to execute any and all document(s) necessary to assure ownership of the Intellectual Property vests in the State and shall take no affirmative actions that might have the effect of vesting all or part of the Intellectual Property in any entity other than the State. The Intellectual Property shall not be disclosed by contractor or its subcontractor(s) to any entity not the State without the express written authorization of the agency, department, division, board or commission of the State of xyz requesting the issuance of this contract.

OR - from a University

3. Policy on Intellectual Property - Copyright; Patents; Inventions; etc.

This section (section 3) applies to all staff.

This section (section 3) is also the policy that applies to postgraduate and undergraduate students in such cases where the University has sole or joint ownership of the Intellectual Property generated by their work.

Intellectual Property is inevitably created as a consequence of University activities. Intellectual Property Rights (IPR) can have a commercial value, which may be exploited for the benefit of the University and staff without in any way compromising the academic commitment to the free dissemination of ideas. The University wishes to encourage the initiative of staff in the creation of intellectual property, and in the identification and exploitation of discoveries. Intellectual property includes patents; copyright; design rights; registered designs; and trade marks. Copyright and design right arise automatically, the others have to be registered in order to be protected (protection applies from the date of application for registration), and fees paid to maintain that registration. Nevertheless it is advisable to label all University-owned works (including material on the internet) as "Copyright © 2000 University of XXXXXX, All Rights Reserved"

The legal position is that all inventions and applications or know-how developed or determined in the course of employment (including copyright, the copyright subsisting in computer programs, and design rights) are the property of the University, unless agreed otherwise. Each member of staff therefore has an obligation to disclose such intellectual property to the University. Staff have a duty in particular to ensure that the invention does not become publicly known (eg through publication or presentation at a Conference or meeting) - and so the right to file a patent application is lost - before a decision has been made within the University on whether or not a patent application should be made, and before the patent application is filed if that is the decision. In return, the University will take reasonable steps to assess whether it would wish to protect and exploit the intellectual property (to the benefit of the individual and the University). If the University decides not to exploit an invention or application, the inventor / originator will be entitled to do so. If the University decides not to exploit the intellectual property the inventor / originator will be informed within 12 months of disclosure of the intellectual property to the University.

IPR may, however, not always belong to the University. Where work, such as research, is carried out for a sponsor, the draft contract may provide that the intellectual property rights in the results will be owned by the sponsor. It is University policy that, wherever possible, ownership should remain wholly or partly with the University. Staff must take account of this when discussing proposals with sponsors, and should take advice from the Graduate Research School before concluding any negotiations.

Now, consider the following;

Where staff are engaged on some routine software development tasks and in the course of their employment they use Open Source software to develop for your business or organization, new algorithms, new executables and new applications that make your business more efficient in the day to day running. It may even be for a new software product that is secret and will be released soon as a world beater!

As they have in-grained in them already (from their university/college education background) they don't think twice about making their Open Source "Contribution" publicly available by uploading to one of the many free software sites the source code for their code segment/changes etc! After all that's what Open Source is all about!

In reality, the problem arises because staff may well sign the above Terms and Conditions (the fine print of which becomes forgotten about very quickly) and yet the golden rules of Open Source will continue to influence their handling of any IP created and override any Terms and Conditions of employment UNLESS you have in place very strong vetting procedures for tracking and recording, management and auditing of the IP.

But, we have a legal agreement!

Now, it's at this point the legal eagles jump up and down and say this can't be, we have a signed agreement with the employee.

True, so you might well have, but when did you check last to see how well protected you are in the scenario outlined above?

It's happening under your nose already far too often and you need to take steps to stem the tide!

This is an assertion we can back up by fact as we have seen a number of organizations (no names will be disclosed) who have no idea about the issue, hence we are sharing it with you!

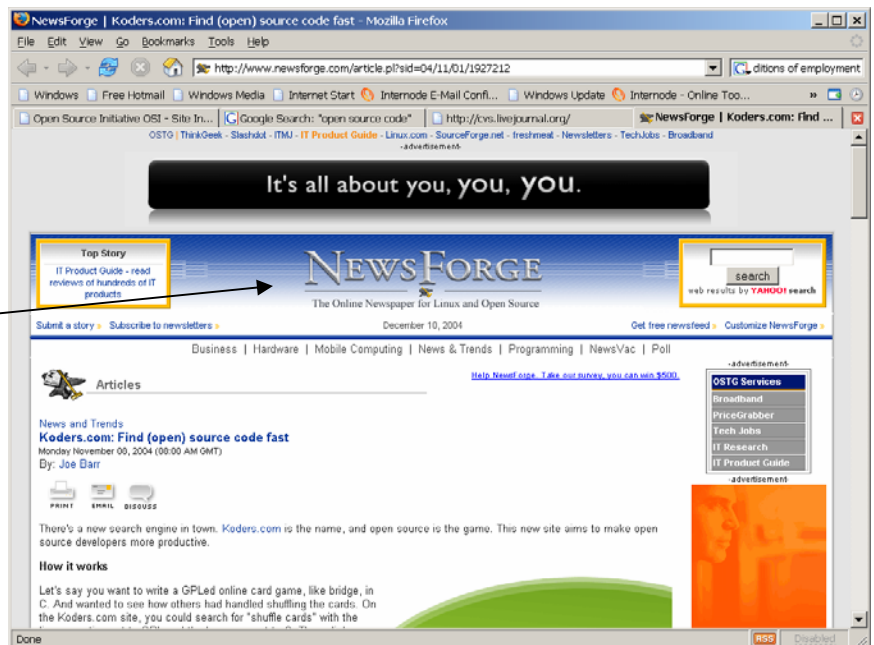
How many Open Source Sites?

If you Google for the words Open Source Code there are nearly 18million!

Narrowing it down to the phrase "Open Source Code" gives 309,000!

There are ample tools provided to help users find Open Source code freely and easily

Sun Microsystems is also about to release a Common Development and Distribution License (CDDL) for Unix on Solaris which is not expected to be compatible with GPL issued by the Open Source Software Initiative. This will further complicate the industry handling of licenses.
Source ARN Dec 15th 2004



What needs to be considered?

When considering IP issues you need to look at the following areas.

Internal IP Records need to include at the very least (to give you MAXIMUM PROTECTION);

- a short form description of the IP being classified and recorded internally
- the nature of the IP right which subsists (whether it is a Patent, Patent application Trademark, Copyright, Published work, Escrow, Deeds, Agreement, Registrations of Idea, Registered Design, Trade Secret / Confidential information etc or an Unpublished work etc)
- a detailed description of the IP (beware of disclosing too much – store some detail securely)
- the name of the author/s and inventor/s;
- the name of the actual owner/licensee of the IP;
- details of any relevant IP applications and/or registrations (including type, number, status {pending, in-force, expired} and country);
- documents for which copyright is asserted, evidence of copyright authorship and relevant dates, including the date of publication of the work or a statement that the work has not been published; and whether the copyrighted work is original or an adapted work and whether published or unpublished.
- The date of IP application, term and renewal dates for any patents, filings, registrations etc

If the IP involves adaptations, and/or enhancements to Open Source software, then the location and consent for the Original work being used and the “Contribution” you have made where changes have been made, needs to be entered into a specially constructed section within the IP register. **Legal advice will need to be (this is a MUST DO) sought from your specialist IP lawyer or legal counsel BEFORE any contributions are "released back" as public domain Open Source contributions!**

Your audit program needs to check to see the above is being maintained in a database register accurately – and that senior management understands the risk and the issues faced in this area. This includes the need for rapid approval of any IP so that it can be recorded, tracked and approved for inclusion on the IP register/s. **Assign the database to a key team of senior management to hold, manage and maintain etc as it is business critical information and should be reported on at least quarterly at Executive Management Meetings!**

The screenshot shows a Microsoft Access window with a form titled "Intellectual Property Register - PATENTS". The form is divided into several sections for data entry. On the left side, there are fields for "IP Register Number - Patents" (with a note "(AutoNumber)"), "Short Title", "Description", "Class", and four "Inventor" fields (Inventor 1 through Inventor 4). Below these are fields for "Owner" and "Licenses (if any)", followed by a "Comments" text area. On the right side, there are dropdown menus for "Patent Status", "Priority", and "Countries filed". There are also input fields for "Filing Date of Patent", "Term of Patent" (with a value of 0), "Renewal date", and "Patent / App. No.". At the bottom of the form, a yellow banner contains the text "Use 1 form for each IP and Patent requirement". The Microsoft Access interface includes a menu bar (File, Edit, View, Insert, Format, Records, Tools, Window, Help) and a toolbar with various icons. The status bar at the bottom indicates "Form View" and "Record: 1 of 1".

TAKE A TIP! You might like to “test the water” to see how far your IP has already leaked out if you have been using Open Source software in your business!

A Helicopter View

IP management in any organization (business or government) needs to be undertaken bearing in mind the following key issues;

- A management commitment must be made at the highest level for protecting, managing, controlling and auditing of IP records and reporting to senior management of IP held
- This commitment must be cascaded to all levels across and throughout the organization (hold regular training/information sessions)
- Organizations don't (generally) willingly, let the IP leak out of the organization however many just have no idea already that it is already happening!
- It's staff at all levels who create the problem for you by not being briefed on the issues and risks etc and not being supervised when it comes to management and release of information
- Organizations who choose or wish to spend the least amount of time and energy on IP management are the losers in the bigger scheme of things and are NOT protected as well as they could be, in fact they may lose their rights to IP due to inadequate management
- Commitments made regarding IP management and process handling must be communicated, often, to all staff in the organization (hold regular information sessions in key hot spot areas)
- All staff must be made accountable for their actions, at all times and employment conditions need to be reviewed by legal counsel to ensure the IP is really locked in
- Most organizations feel that recording and tracking IP followed by conducting compliance audits are a waste of time and money, so auditors will need to "stand up and champion the cause" to ensure that adequate protection is given to this business critical information – your survival depends on it!
- **IP Recording and Tracking and Compliance audits are a necessary functional act that must be endured to protect your position, your assets and your corporate knowledge and market position!**
- **Open Source Software and "Contributions" presents some very unique IP leakage issues that need your attention today!**



Turn the TAP OFF!

DON'T LET YOUR ORGANIZATION LOSE IP WHEN USING OPEN SOURCE!

This article written exclusively for AUDITNET.ORG by: PCProfile and 1st published in December 2004 by Rob Harmer Consulting Services Pty Ltd P.O. Box 196 Modbury North Sth Australia 5092
Phone +61 (0) 418 817 955 fax +61 8 8265 1961

PC Profile is Australia's ONLY anti-piracy (self-help / non-policing) advisory service and solutions provider based in Adelaide, Sth Australia email: rharmer@internode.on.net web site <http://www.pcprofile.com>

This article and contents Copyright © 2004 All Rights Reserved Worldwide Rob Harmer Consulting Services Pty Ltd