

SOFTWARE LICENSE COMPLIANCE AUDIT

Audit Report No. SC0106

August 15, 2006



**MENTAL HEALTH MENTAL RETARDATION
AUTHORITY OF HARRIS COUNTY**

Internal Audit Report

AUDITOR'S REPORT

Software License Compliance Audit

Harris County, Texas

Internal Audit Report

August 15, 2006

Henry E. Webb, CFE

Internal Auditor





August 15, 2006

Steven B. Schnee, Ph.D.
Executive Director
MHMRA of Harris County
7011 SW Freeway
Houston, TX 77074

RE: Software License Compliance Audit
Audit #SC0106

Dear Dr. Schnee:

BACKGROUND

Software Legitimacy

In simplistic terms, Information Technology's (IT) mission is to operate, maintain and safeguard the Agency's telecommunications, data networks and core network services; to plan, acquire, operate and maintain software applications and their server platforms on behalf of MHMRA departments; to plan, operate, support and maintain the desktop/laptop workstations and core productivity software for the Agency staff; to plan, support and safeguard the utilization and maintenance of Agency data.

The IT Department provides test equipment and software systems to monitor server operating parameters and utilization as well as software for central deployment. The support or technical staff provides the installation, support, and maintenance of desktop/laptop for users. The staff provides support for users at their locations, as well as training on software applications.

Agency policy does not allow staff to install or download software without the permission of the IT Director. MHMRA's IT Department has also restricted or locked down most desktops and the Internet to make this policy easier to enforce. Further, the Agency tracks all software purchases through the use of either the software application Track-It or Software License Tracker by CDW Healthcare. Furthermore, software purchases that are over \$5,000 and have a yearly maintenance agreement (Fixed Asset Requirement) are also tracked in AssetWin, the Agency Fixed Asset database.

Agency Application Software

MHMRA of Harris County's main "tool" to maintain control over software installation count is the application software called Track-It, as well as Software License Tracker by CDW Healthcare. These applications provide an array of uses that allow the Agency to install, remove, update and repair software applications, as well as track the software by computer location, owner, etc.

MHMRA of Harris County has purchased approximately \$3,078,347 in software and spends approximately \$330,000 per year for software maintenance agreements.

Software Assets

Software assets will usually fall into one of three basic categories:

- 1) **Software Licenses** – these licenses may permit the Agency to make individual installations of a particular product or to install that product site wide at a particular location.
- 2) **Physical Media** – in some cases media and licenses are one in the same, and often times companies don't make their products available for download so it can be very important to track the media that the Agency has for various products.
- 3) **Maintenance Contracts** – although not always directly related to the installations (the Agency may install software for products even though they do not have a support contract for the product), maintenance contracts often imply/include the right to upgrade to new versions for the duration of the contract and, even when these are limited to support, comprise an important part of the conditions under which the license provides use of the software.

License Type

The primary indicator of how software license relates to the software installations is by license type.

- **User Licenses** are used to indicate that the software is licensed, not surprisingly, one per user. Typically if you have 50 user licenses of a product then you have a license to install as many of that product to the various computers that you manage. This is one of the most common licensing methods.
- **OEM Licenses** are licenses which are bundled with the computer at the time of purchase by the OEM (Original Equipment Manufacturer). Typically these licenses cost significantly less than the full retail version of the same product or operating system, but can only be used on that particular machine.
- **Site Licenses** are another common method of licensing software. In the case of site licenses, rather than requiring a separate license for each separate instance of the software that is installed, the Agency may hold a license to install and use as many copies of the software as they like, either at a particular location (site) or across the unit.
- **Proprietary Licenses** refers to any licenses where the software is licensed by the publisher in a proprietary fashion and may include its own proprietary license management system. An example may be the ENT Server itself. The technicians/managers that use the ENT Server can access this via either a web browser (which requires no installation of the software) or other means which allows them to install and use as many copies as necessary – all over the network. In this case, the software (ENT Server) comes bundled with tools to help manage licenses for the ENT Server and ensures the proprietary license requirements of the software so that the Agency never uses more licenses than it owns.
- **Freeware Licenses** are typically a carte blanche to install/use as many copies of a particular piece of software as the Agency may desire.

Penalties

Private monitoring organizations, formed by software companies such as Microsoft, Autodesk, Adobe, IBM, Intel and others, can gain access to a business premises to learn whether computer programs such as Microsoft Word have been illegally copied or “pirated.”

One of the monitoring organizations, the Business Software Alliance (BSA), defines software piracy as “the copying, distribution or downloading of unauthorized copies of software.” The two most common forms of software piracy are:

- **End-user copying:** Organizations installing software on more computers than are licensed or friends loaning disks to each other
- **Distribution:** Duplication and distribution of illegally copied software, including counterfeit products

Armed with the power to enforce their members' software copyrights, these monitoring organizations set up telephone hotlines and web sites where people (often disgruntled employees) can report purported software license violations anonymously.

Computer software is protected by the U.S. Copyright Act. 17 USC &102 (a) (1); 1 Nimmer on Copyright, Subject Matter of Copyright, &2.0 [c], p. 2-51 (2003). The Copyright Act provides for damages, civil penalties and attorney fees for copyright infringement. An infringer is liable for either the copyright owner's actual damages and profits of the infringer or statutory damages of \$750 to \$30,000 for each work infringed. 17 USC &504 (a), (c) (1). To recover statutory damages in most cases, the infringed work must have been registered with the Copyright Office before the infringement. 17 USC &412.

If the copyright owner can prove that the infringement was willful, the court has discretion to increase the statutory damages to \$150,000 per work. 17 USC &504 (c) (2). The court also has discretion to impound all allegedly infringing copies of the work at any time while the action is pending. 17 USC &503 (a). As part of a final judgment or decree, the court has discretion to order destruction of all infringing copies. 17 USC &503 (b).

The Courts also have discretion to award the prevailing party its cost of suit. And, if the work was registered with the Copyright Office before infringement, the prevailing party may be awarded its attorney fees. 17 USC &&412, 505.

Besides civil enforcement, many monitoring organizations work closely with federal law enforcement agencies. Copyright infringers are subject to criminal penalties. If the infringement was willful and for purposes of commercial advantage or private gain, first-time offenders face up to five years in prison and subsequent offenders face up to 10 years in prison. 17 USC &506 (a); 18 USC &2319. Individual infringers also face fines of up to \$250,000, and infringing organizations, such as corporations, face fines of up to \$500,000. 18 USC &3571 (b), (c). These criminal fines can be even higher if the infringer derived a pecuniary gain or the infringement resulted in a pecuniary loss to another. 18 USC &3571 (d).

It is estimated by one of the monitoring associations that the world software industry lost approximately \$13 billion in revenue in 2002 because of software piracy. In the United States in 2002, it is estimated that the software industry lost not only \$2 billion in revenue but, also, 105,000 jobs, \$5.3 billion in wages and \$1.4 billion in federal and state tax revenue.

In August 2002, the Business Software Alliance announced that it had collected \$5.8 million in settlements so far that year and had reached 44 new settlements totaling \$3.1 million.

OBJECTIVES

The overall objectives of the audit were to determine whether the departments:

- Managed and used resources in an efficient, effective, and economical manner
- Administered funds in compliance with applicable laws, regulations, policies and procedures
- Implemented internal controls to prevent or detect material errors and irregularities

The specific objective in this audit was to:

- Assist management with the assessment of the adequacy of internal controls related to recording, reporting, and safeguarding the Agency's control over computer software installation compliance with applicable licensing requirements.

SCOPE

The scope of the work did not constitute an evaluation of the overall internal control structure of the units. The examination was designed to evaluate and test compliance with established policies and procedures and to test the internal control over tested areas and material. The audit scope was limited to confirmation of software programs with corresponding licenses available.

Department management is responsible for establishing and maintaining a system of internal controls to adequately comply with approved policies and procedures. The objectives of an internal control system are to provide management with reasonable, but not absolute, assurance that assets are safeguarded against loss from unauthorized use or theft, and that transactions are executed in accordance with management's authorization and are recorded properly.

Because of inherent limitations in any system of internal accounting control, errors or irregularities may occur and not be detected in a timely manner. Also, projection of any evaluation of the system to future periods is subject to the risk that procedures may become inadequate because of changes in conditions, or that the degree of compliance with procedures may deteriorate.

The purpose of the audit report is to furnish management independent, objective analyses, recommendations, and information concerning the activities reviewed. The audit report is a tool to help management discern and implement specific improvements. The audit report is not an appraisal or rating of management.

Although due professional care in the performance was exercised, this should not be construed to mean that unreported noncompliance or irregularities do not exist. The deterrence of fraud is the responsibility of management. Audit procedures alone, even when carried out with professional care, do not guarantee that fraud will be detected. Specific areas for improvement are addressed later in this report.

Other minor findings, not included in this report, have been communicated to management and/or corrected during the audit process. Internal Audit would like to thank management and staff for their cooperation throughout the audit.

METHODOLOGY

In order to meet the objectives, Internal Audit evaluated controls over computer software installation compliance with applicable licensing requirements, and reviewed policies and procedures for compliance and completeness. MHMRA staff was interviewed and audit tests and procedures were conducted as considered necessary.

The sample size and selection were statistically generated using a desired confidence level of 95%, expected error rate of 5%, and a desired precision of +/-5%. Statistical sampling was used in order to infer the conclusions of test work performed on a sample to the population from which it was drawn and to obtain estimates of sampling error involved. When appropriate, judgmental sampling was used to improve the overall efficiency of the audit.

STATEMENT OF AUDITING STANDARDS

The audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that Internal Audit plan and perform the audit to afford a reasonable basis for the judgments and conclusions regarding the organization, program, activity, or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws and regulations when necessary to satisfy the audit objectives. An audit also includes assessing the estimates, judgments, and decisions made by Agency management. It is believed that this audit provides a reasonable basis for the findings, conclusions, and recommendations.

RESULTS

As a result of the audit procedures and surveys conducted, it was determined that departmental compliance with either established or drafted criteria to govern control over computer software installation compliance with applicable licensing requirements is adequate. However, it was discovered that certain internal controls need to be strengthened. These and other items are discussed below.

FINDING

Policy and Procedures

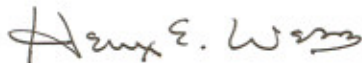
MHMRA of Harris County has in place a set of policies and procedures that govern the use of fixed assets and inventory equipment. As part of these policies, MHMRA requires that *"The Laptop Computer Agreement must be renewed annually."* **BUS-R/I:10.1** One area of weakness noted during the review was the laptop computers. They may be quarantined from the network, and consequently, IT's network management software cannot detect what programs may be on those machines.

Recommendation

- It is recommended that IT Management draft a policy and procedure that specifically addresses the need to inventory the software residing on Agency equipment at least annually (to include laptop computers – logically at required annual renewal time).
- It is further recommended that the policy and procedure include the following required reports:
 - * Software installed (software installation audit)
 - * Agency owned software (software asset audit)
 - * Compare software installation report to software owned report

Management Response

"IT agrees with recommendations and will begin immediately to draft such a policy. IT also suggest that Purchasing properly record new software license into the ROSS System as a cross check on Agency-owned software."



Henry E. Webb

Cc: Rose Childs, MSW, CSWM, Deputy Director, Mental Health Division
Kenneth Collins, LMSW, Deputy Director, Mental Retardation Division
Barbara Dawson, MSE, Deputy Director, Comprehensive Psychiatric Emergency Program Division
Avrim Fishkind, MD, Medical Director, Comprehensive Psychiatric Emergency Program Division
Sarah Flick, MD, Medical Director, Mental Retardation Services
Sylvia Muzquiz, MD, Medical Director, Mental Health Services
Jeanne Mayo, MS, JD, General Counsel
David Witt, MPA, CPA, Chief Financial Officer
Eric S. Eaton, CPA
Audit Committee:
Tom Hamilton, Ph.D. (Chairman)
Jane B. Cherry
Paige M. Cokinos
Charles O. Buckner, CPA
Vicki S. Raynold, CPA
Bob Borochoff

ATTACHMENT A
SUMMARY OF RECOMMENDATIONS
August 15, 2006

Unit: IT Area: Software Compliance		
Inherent Risk: Low Moderate High	Control Environment: Well Controlled Acceptable Poorly Controlled	Overall Risk: Low Moderate High
Type of Procedures: Audit		
Scope: <ul style="list-style-type: none"> * Using Internal Control Evaluation (ICEs) forms, documented the internal controls * Conducted a preliminary survey reviewing applicable policies and procedures, etc. * Interviewed various staff to obtain understanding of management controls * Examined detailed invoices/work orders, statements provided by the vendor, etc. 		
Priority Rating: 1	Audit Recommendations: Specific Policy and Procedures be developed to address software inventory	
Follow-up: 1 year		

Priority Rating

1. Implement immediately (30 - 90 days) - Serious internal control deficiencies; or recommendations to reduce cost, maximize revenues, or improve internal controls that can be easily implemented.
2. Work towards implementing (6 - 18 months) - Less serious internal control deficiencies, or recommendations that can not be implemented immediately because of constraints imposed on the unit (i.e. Budgetary, technological constraints, etc.).
3. Implement in the future (2-3 years) - Recommendations that should be implemented, but that can not be implemented until significant and/or uncontrolled events occur (i.e. legislative changes, buy and install major systems, or require third party cooperation, etc.).