Overview, challenges and remedies of software license compliance

A white paper by NASSCOM and
EY Forensic & Integrity Services

NASSCOM®

EY
Building a better
working world

Introduction

A software license is a legal instrument that provides for use of the software with specific terms and conditions. When proprietary software is bought, only the license to use it is bought. The proprietary rights, however, remain with the software publisher.

Software has become crucial for any business in today's world. With the ever-increasing dependency on software and investments on the rise, it is very important for a company to have proper controls in place to manage its software environment.

With products and solutions emerging from India, it is important that the industry is aware of the necessary safeguards in licensing to mitigate any misuse and infringement of their intellectual property.

For a licensee organization, investments in software are huge and carry the burden of maintenance, which is a recurring cost. On the other hand, software support and maintenance fees account for the major source of revenue for software publishers.

Another revenue stream for publishers today is compliance audits, as they allow for upselling. As a result, publishers today are driving software compliance audits for their end customers more aggressively than ever.

Typically, an organization faces an average of three compliance audits per year. Any compliance audit will take two to three months to complete and requires significant time and effort on the part of companies. Compliance audits would generally lead to the identification of:

- Over-deployment of software
- Presence of pirated or cracked software

This situation could change a friendly compliance conversation to a rather disagreeable situation.

It is therefore important for both licensors and licensees to incorporate proper controls in place to check the use of an organization's software assets. This should be done to not only avoid financial setbacks, but also reduce reputational risks for infringing entities.

This whitepaper provides insights into the various risks related to software non-compliance, how it can arise, the major challenges that companies are facing today and what they can do to maintain a good software license compliance position.

Gartner insights:

- ‣ Gartner predicts that overall spend on software is expected to increase to **US$326 billion** in 2016 from **US$310 billion** in 2015

- ‣ Gartner also estimates that data center investments will account for **54%** of overall spend

Factors leading to non-compliance

The following are some of the key factors that often lead to IP infringement. These, if neglected, have the potential to result in non-compliance for licensees and revenue loss for licensors.

License overuse

Overuse is not limited to deployments only. Lack of proper accounting or use outside of the terms and conditions of the license agreement can also lead to overuse of licenses. Further, sharing of user accounts, concurrent use, cross-border use, unmanaged virtualization and access to third-party applications may also lead to overuse.

Complexity of software license contracts

Contractual license agreements are complex and require proper attention at the stage of negotiation as well as after implementation. The terms and conditions of a contract can be vague and would require proper interpretation to comply with license usage. A vague agreement can result in confusion in terms of usage of licenses and may pose legal as well as financial risks to an organization.

Cracks, keygens, rogue codes and pirated software

Organizations often fail to identify the presence or usage of cracks, keygens and rogue codes in their environment due to lack of expertise and advancements in piracy; these may have been downloaded by a rogue employee or vendor. Today, with companies increasingly allowing their employees to access company information through their own devices, the risk further aggravates.

Challenges related to virtual environment

Maintaining licenses under a virtualized environment can be a challenge. Virtualization requires applications to be run on shared hardware resources. This makes it difficult for organizations to differentiate and measure hardware and software deployed in a virtualized environment, thereby increasing the risk of non-compliance.

Indirect access by third-party applications

In case of companies using complex software, the information has to pass on from the web portal to the software such as ERP when their customers make online purchases. Publishers may view this as indirect usage and require additional licensing for it.

Sharing of user accounts or multiple logons

At the time of implementation of an ERP system, multiple logon scenarios are allowed to update records to inventory and other modules. This is generally allowed keeping in mind the business requirement of getting the system up and running soon. After implementation is over, these multiple logons need to be checked. When publishers conduct license audits, these multiple logon cases, if still continued, could result in non-compliance on account of password sharing and violation of named user licensing terms.

According to BSA Global Software Survey 2016, **39%** of software installed on computers around the world in 2015 was not properly licensed, representing only a modest decrease from **43%** in BSA's previous global study in 2013.

BSA's survey Seizing Opportunity Through License Compliance (2016) found that in India, **58%** of the software installed on computers not properly licensed.

Incorrect user license allocated based on roles and departments

Users are given access based on the role they perform in the organization. Often, users are classified and licensed based on the access they have on the system. "Create," "update," "edit," "view" and "delete" are the prime categories of access granted. If all users have the rights to "create" or "update," then they may be required to be licensed under the highest category, resulting in unforeseen revenue loss to the organization. Hence, it is very important to regulate and control accesses for all users and also to categorize them properly to maintain compliance.

Bundling restrictions from publishers

Software publishers sell some of their licenses in bundles, which have their own terms and conditions attached. Some bundled software is allowed to be broken, and individual components can be used as regular products, while some have limited use restrictions. There are certain bundles that cannot be broken. If such usage is not monitored, this could result in non-compliance. A similar situation arises when companies deploy multiple copies of the software for disaster recovery and business continuity.

Installation traces

Organizations need to do a clean uninstallation of software and license keys that have expired or are no more in use. Installation traces and leftovers after uninstallation of expired software or used software can often be misinterpreted and lead to disputes with publishers during an audit.

Cross-border usage

Using licenses remotely between countries and offices can lead to non-compliance. Generally, most software license agreements restrict use outside of the country of purchase. In case of a global organization, having offices across different countries, it is possible that licenses purchased in one location are used in another. These organizations may end up paying extra for such global deployment cases.

Expecting IT department to be the sole owner of compliance

Even today, the common perception is that it is the IT department's responsibility to maintain compliance. Rogue users may try out different things to breach compliance levels. Awareness campaigns are generally ignored by employees. This mindset needs to change and individual users should own the responsibility for compliance. Therefore, IT should involve finance, legal, procurement and user groups to manage compliance. These things may appear trivial, but end up costing the company significantly during compliance audits.

A survey from Gartner has highlighted the license compliance audit trends of the top five publishers during 2009–14:

6-Years Vendor Audit Analysis

Legend: SAP, Oracle, Adobe, Microsoft, IBM
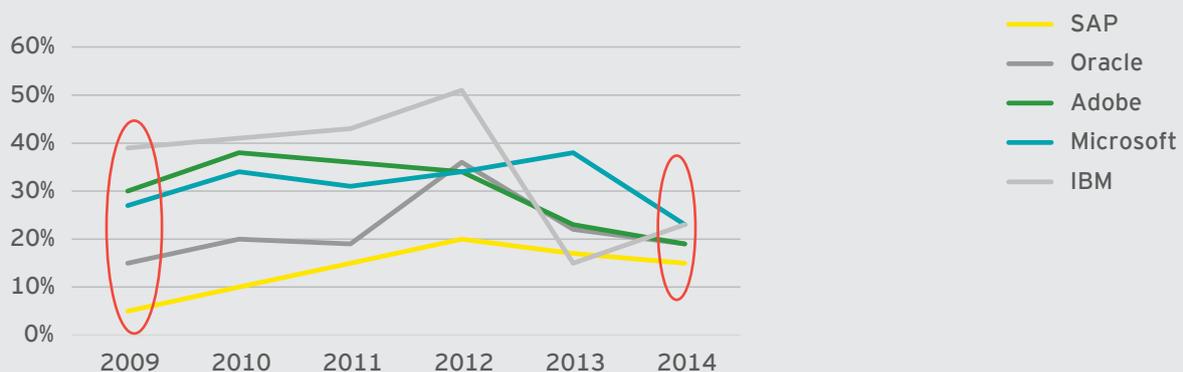
Challenges related to software licensing

Software licensing is a complex topic and the entire process of software license management – from purchase, deployment and maintenance to disposal – can be challenging if the licensing details are not well understood. Some of the major challenges related to software licensing are highlighted below:

Ambiguous contracts

Software contracts are complex and span multiple versions over decades. Complicated terms and conditions coupled with legal language tend to make them difficult to interpret and understand. The complexity further increases when crucial terms such as indirect access to ERP software, licensing based on employee, CPUs and asset size become difficult to identify and quantify.

Unplanned procurement

Forecasting purchases requires a lot of planning. Determining the correct quantity of licenses to purchase requires precise information about current entitlements and future growth plans. A company would be able to make a sound purchasing decision only when it has accurate and up-to-date information and a planned approach to procure software.

Management focus

In most cases, companies end up paying huge penalties to publishers because of the fact that they do not invest sufficient time and effort in educating their employees about risks of non-compliance. Gaps in management focus pertaining to non-compliance can lead to significant repercussions.

Purchase program options

Deciding what to purchase, when to purchase and how to purchase is a major challenge for organizations. With a wide array of purchasing options such as perpetual licensing, unlimited licensing, subscription-based licensing, true-up and burn-down options, it could become difficult for companies to decide on which option they should go for.

Lack of Internal controls and automation

Lack of internal controls relating to tracking of compliance and prohibiting the use of unauthorized software and insufficient infrastructure to check data leakage can lead to significant financial exposure. Further, tracking software license compliance cannot be a manual exercise, as the IT environment for most companies is dynamic and changes drastically in a matter of days. Automation and use of technology are the most important aspects in enabling proper governance and control.

Low understanding in the developer community on scope and open source obligations:

Developers use various software for development purposes.

- Open source: Generally, developers have the permission to access and download various software, especially open source. When developing software, open source software may be used. Not all open source software is free of charge. Developers need to be cognizant of the nuances of open source license terms and conditions.

- Trial version: Many software programs are available on the internet as trial versions. If use is continued after the trial period, the software becomes chargeable. Organizations should therefore have proper controls and frameworks in place to manage the software programs that are being used for development to avoid infringement of copyrights.

Sometimes, trial or test versions of developer tools cannot be used to develop commercial offerings. For instance, a company developing a software using a trial or test version should check that the underlying software is properly licensed and has the correct commercial terms before offering the end product for sale. It should also consider indemnity coverage for any third-party claim on the developer tools.

New licensing models

Apart from the traditional perpetual licensing models (which used to generally be on a per user, per CPU, per instance or per virtual machine basis), technological advances have brought in new services, which are broadly termed as "cloud" or "cloud computing." Cloud computing includes various services, such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). The payment in these services is generally on a "pay-as-you-use" basis and is also called as "subscription licensing."

In India, there has been a rapid adoption of cloud computing and cloud-based infrastructure in the past couple of years. Many publishers now offer their traditional software products in a cloud-based environment covering both hardware and software for a subscription fee. However, organizations need to be careful while moving applications to a cloud setup. Applications that have a sizeable amount of interplay between the organization and the external world, software that has periodic peaks of use and software that is dependent on internet access are ideal to be moved on to a SaaS model. On the other hand, applications where speedy processing of data is required or where legal contractual terms limit hosting of data externally may not be suitable for a SaaS model.

Further, as Indian companies increasingly develop cloud-based offerings, they need to develop and design robust cloud-based licenses, including on demand licensing models.

Maturity levels of software license compliance in India

Our assessment has covered various companies in India and looked at the on-ground situation across industry sectors. We have evaluated the maturity levels taking three factors into consideration:

Cracks and keygens: This indicates the presence of cracks and keygens, which can lead to the use of cracked software

Non-compliance with license-related rules: This indicates non-compliance relating to overuse – buying X and using more than X.

Wastage: This indicates wastage of licenses due to incorrect tracking or budgeting or unused old versions

Magnitude of issues found – the larger the issues, the lower the maturity

	Banking	IT/ITeS	Manufacturing	Pharma	Real Estate	Telecom
Cracks and keygens	20%	35%	52%	5%	30%	40%
Non-compliance with license-related rules	45%	53%	69%	25%	27%	32%
Wastage	25%	25%	20%	5%	15%	20%

Legend: ■ Cracks and keygens ■ Non-compliance with license-related rules ■ Wastage ― Maturity Level
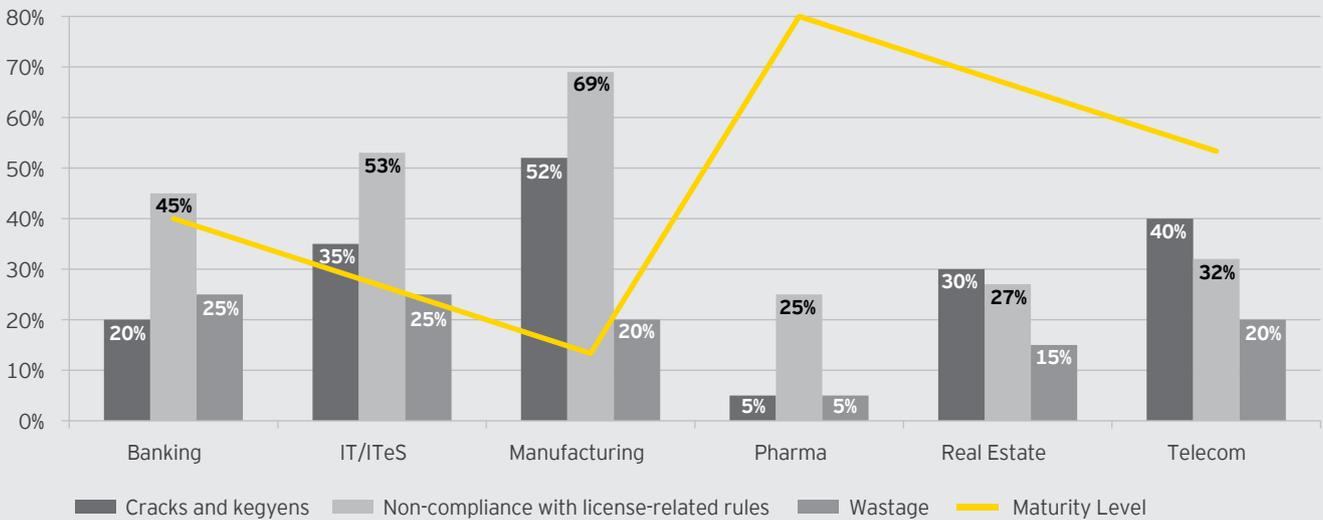
Source: EY research

Global leading practices: What needs to be done?

In the light of the various challenges around software licenses outlined above, organizations should strive to engage in proper planning, education and technological assistance to combat the risk of non-compliance. A shift in approach and attitude would help companies maintain an optimized and compliant license environment. Below are some of the leading practices that can help organizations maintain compliance:

Management involvement

Follow a top-down approach to bring about changes to the software compliance mind-set in an organization. Employees will get serious about software usage and compliance only when they know that there is a strong focus from the management.

Being proactive

Use processes and controls to track software usage and compliance that are at par with industry standards. Start now!

Centralized purchasing of licenses

Create a central repository of all entitlements to know what you have and be better enabled to make purchasing decisions. Purchases should be made centrally to gain benefits of volume purchases.

Know your contracts

Involve the legal and technical teams during the discussion phase, before signing contracts. It is important to know what you are signing up for. After implementation and during use, check that the licenses are being used according to the terms and conditions outlined in the contract.

Periodic internal audits

Perform periodic internal software audits to help understand the compliance position. In addition, capture the deployment of all software being used in your environment.

Cracks and keygens identification

Build expertise around the detection of cracks and keygens, try to identify how these got into the system and take protective measures. They should also identify employees using cracked keys and take necessary steps. This would send out a strong message to all employees for enhanced compliance.

Roadmap for future

Forecast software license growth and have an effective purchase plan for your organization. It is crucial to remember costs will only increase with time.

Software policy

Have a software usage policy in place and have it read and signed by all employees periodically. The focus should be on creating awareness among employees about the importance of software assets and their usage.

Software bundling

Be cautious about the usage conditions from different publishers around software bundling.

Technology enablement and automation

Deploy specialized tools and technologies to help automate the discovery and reporting of compliance.

Skill development

Deploy specialized tools and technologies to help automate the discovery and reporting of compliance.

Myths vs. facts

Myths related to compliance with software license rules

Myths

- No documentary evidence maintained of software purchases

- "We have volume license, we are compliant...."

- License compliance is only IT team's responsibility

- "We won't get audited."

- Software is installed but not in use

- No one will know if software is installed

Facts

- If you own it, prove it

- Provides flexibility for purchase, with standard audit clauses

- Tracking software license not on priority list – license spraw

- Everybody gets audited

- In most cases license is required for deployment/ installation

- Software may send phone-home signal to publisher if inappropriate usage is detected

Conclusion:

Software license compliance has become an important aspect of businesses. Serious attention has to be paid in maintaining software license compliance, both as a licensee and as a licensor. Software usage, if undetected, can potentially lead to huge penalties and financial losses during publisher audits. Organizations need to be aware of the various aspects of compliance and the different areas that can lead to non-compliance.

Today, software compliance is not a choice for any organization but it is in their own interest to remain compliant of the various risks mentioned here. Further, while it is important for organizations to strike a balance between their license requirements and cost saving, they should not compromise on software compliance, even if there are certain perceived benefits. Focus and commitment by all stakeholders and not just IT will enable respect and enforcement.

About EY's Forensic & Integrity Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

Contact

Arpinder Singh
Partner and Head - India and Emerging Markets
Direct: + 91 12 4443 0330
Email: arpinder.singh@in.ey.com

Harshavardhan Godugula
Partner
Direct: + 91 40 6736 2234
Email: harshavardhan.g@in.ey.com

Ranjeeth Bellary
Associate Partner
Direct: + 91 22 6192 0172
Email: ranjeeth.bellary@in.ey.com

About National Association of Software and Service Companies (NASSCOM)

The National Association of Software and Service Companies (NASSCOM) is the industry association for the IT-BPM sector in India. It was set up in 1988 and registered under the Indian Societies Act,1860. A not-for profit organisation funded by the industry, its objective is to build a growth-led, sustainable, technology and business services segment in the country. NASSCOM's membership has grown over the years and currently stands at over 2200. The member organisations represent 95 per cent of industry revenues and have enabled the association to spearhead initiatives and programmes to strengthen the sector in the country and globally.

NASSCOM has also contributed to the development of two organisations - the Data Security Council of India, which is focused on security and the NASSCOM Foundation, which helps drive Corporate Social Responsibility (CSR) initiatives. NASSCOM is headquartered in Noida, India, and has offices in eight other cities—Bengaluru, Chennai, Hyderabad, Kolkata, Mumbai, Pune, Thiruvananthapuram & Kochi.

Contact

Deepak Arora
Email: policyquery@nasscom.in
Tel: : +91-120-4990111

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

ey.com/in

@EY_India   EY|LinkedIn   EY India   EY India careers