

WHITE PAPER

Risk and Compliance Management in Software Procurement



- Siva R

Abstract

Avoiding risks and eliminating compliance issues in software procurement and management have been the most difficult challenges for CIOs and CPOs all over the world. This paper provides realistic solutions in times of software vendor audits and potential legal issues.

Case In Point

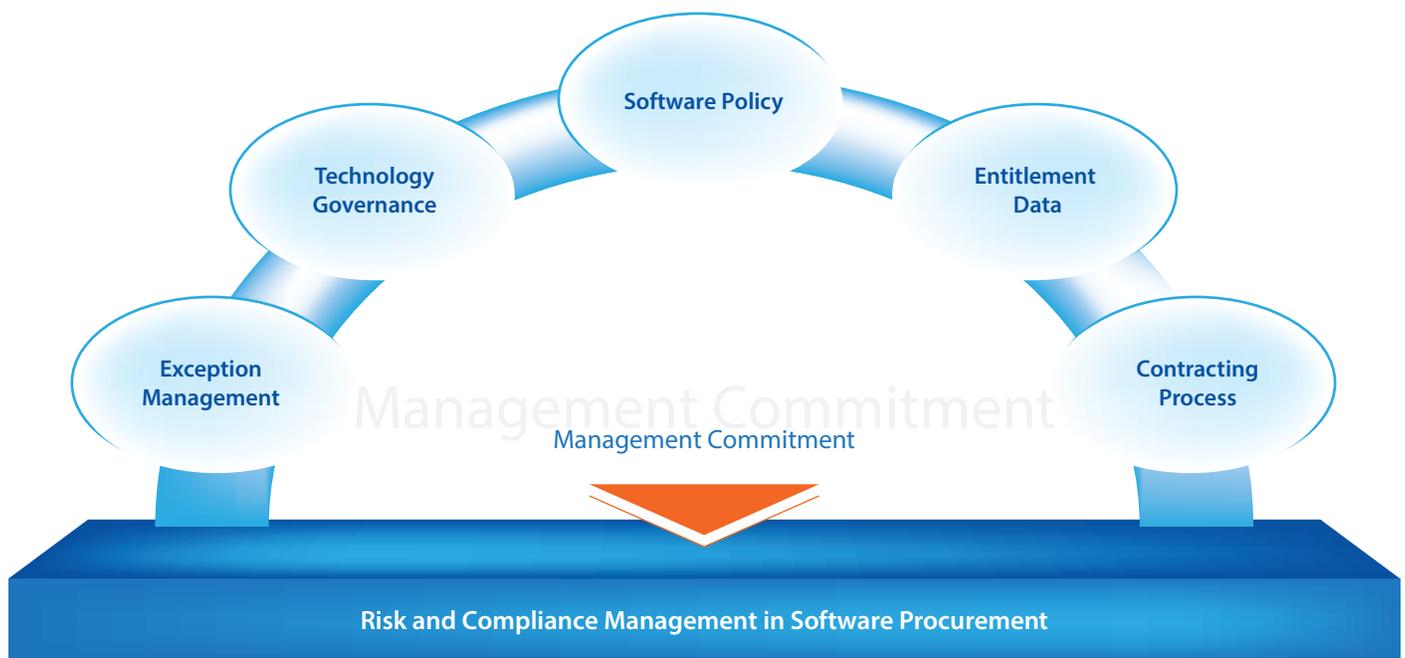
An organization has invested more than \$ 2 Million in implementing a 'best in class' software asset management (SAM) tool. The senior management has approved this investment with a forecasted return on investment (ROI) of 3. The following was the outcome after several months of implementing a SAM program:

- Software Asset Management team continues to struggle in reconciling and optimizing the software licenses.
- There is no clarity regarding the entitlement data for many of the widely used software applications.
- Sensing potential issues, software vendors continue to insist for compliance audits and vendor penalty threats come out large.
- There is a total cost spiral instead of positive ROI.
- Senior management has started

rethinking about the viability of the program.

The above issues have been found to be common across several organizations where a lack of focus in adequate planning and related shortcomings have resulted in chaos and depletion of scarce resources.

Key Elements



Source: Infosys BPO Research

A 'well-conceived' Software Policy

Lack of a software policy leads to multi-dimensional challenges in every organization. Software policy should cover both licenses and services. How the policy should be governed and administered must be clarified to all the relevant stakeholders across the organization.

Best-in-class organizations have separate policies for software that come under 'End User License Agreements (EULA)' and other software that are covered by Master Licenses and Services Agreements (MLSA).

Applications that are procured using EULA create bigger challenges to both CPOs and IT managers since the organization has little control over the terms and conditions that govern these agreements.

The policy needs to highlight the approach towards software resellers. If the software

purchase agreements with resellers do not include the publishers, compliance issues get complicated. Hence, a tripartite agreement covering the customer, reseller and the publisher safeguards the interests of the buyer organization and minimizes challenges.

Process for Software Entitlement Data Collection

Investing in 'high-end' technology tools to collect the installed counts of software licenses will not serve the purpose of reconciliation and optimization, unless a reliable entitlement data is available for comparison. It was observed that most of the failures in a typical SAM project are related to non-availability of 'purchased' software licenses with the procurement organization.

The conventional methodology of

maintaining copies of software license agreements and purchase orders would be laborious and may not yield desired results. Since the software applications are purchased over a period of time and upgraded from time to time (still maintaining copies of older versions in some locations) this process becomes more complex.

The ideal way to get the most accurate data related to entitlement is to 'completely' automate the process by including mandatory fields in the purchase orders that would contain information like license type, license quantity, product name, manufacturer SKU number, license expiry date etc., that can be retrieved in the form of a report and analyzed 'on-line' at any time.

A typical template used for software entitlement data collection is illustrated below:

Sl. No.	Software Description	Quantity	Unit of Measure	Price	Manufacturer SKU	Product Type	License Type	License Quantity	License Start Date	License Expiry Date
1										
2										
3										
4										





Process of Software Contracting

A well-documented software contracting process helps the end users, requesters and the buyers to be conversant with the process that has to be followed and understand the responsibility of various stake holders in the entire process. A visual representation in the form of a process flow diagram simplifies the understanding for user functions and also minimizes potential compliance issues. Typically, software contract processing document is the result of a collaborative effort among the purchasing, legal and IT functions and would require senior management 'signoff' before implementation.

Software contracts start with a Master Licenses and Services Agreement (MLSA), followed by several sub agreements, amendments and work orders. A

comprehensive due diligence is carried out by the compliance team and appropriate recommendations are made before finalizing a Master Agreement. Entering in to a direct software purchase agreement without a Master Agreement can be a high risk engagement and could lead to potential legal pursuits. Some of the best in class organizations adopt 'product specific' or 'service specific' NDAs before initiating a formal RFX process with the potential bidders.

Technology Governance Review

This process is owned by the CIO's organization and involves review and approval of all new software applications that are needed for the organization. The technology governance team maintains an inventory of applications that are currently

used in various parts of the organization along with the relevant usage information. In case of a new request, they verify the availability of a similar application within the organization, its suitability and technical viability and analyze potential threats associated with those applications.

The technology governance review process has been automated in many 'best in class' organizations and the users are suggested to submit their requests through a work flow tool that is typically linked with the software procurement tools. The users would fill in the necessary data in the standard template and the overall approval process gets completed as per the mutually agreed SLAs between the technology governance team and the purchasing organization.

Software Exceptions Management

There is a need for a detailed exception procedure to address various risks and mitigate them in an appropriate manner. The “Shrink-Wrap” or “Click-Wrap” products pose significant challenges to the organization. These challenges mainly arise due to very limited confidentiality of purchaser’s information, limitation of liability and no warranty protection.

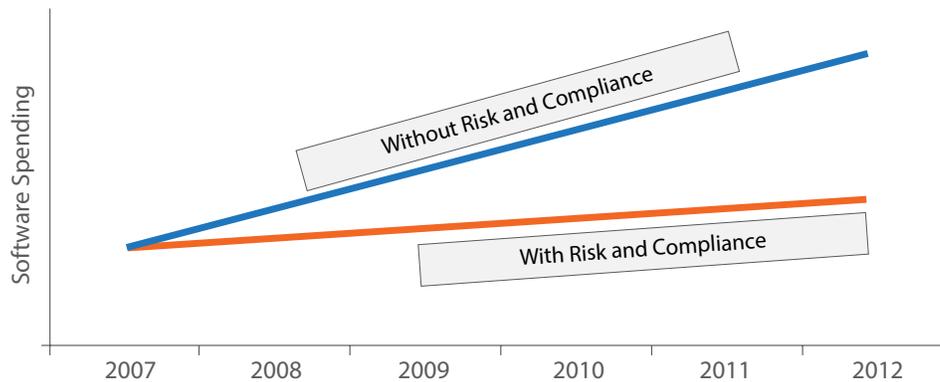
In spite of the above mentioned challenges, there can be a strong business need to go for such applications for sustaining

various business functions. If unique risks are present in any of the shrink-wrap purchases, the risks are clearly identified and documented. In such cases, amendments are proposed to the shrink wrapped agreements to mitigate risks. Acceptance of these amendments by the vendors depends upon the bargaining power and the size of the organization.

Whenever the amendments are not accepted by the vendor and alternate products are unavailable, the documented

risks are submitted to the senior management along with necessary justification for exception approvals. The risks arising out of such exceptions are typically owned by the business owner who takes a decision to go ahead with such software products.

The following graph highlights the cost benefits of enforcing a comprehensive Risk and Compliance Management program in a typical organization:



Source: Infosys BPO Research



Conclusion

Organizations can achieve the following benefits by applying the various strategies described in this paper:

- Quantum jump in contract compliance related to software
- Anytime readiness to face software audits
- Visible improvement in process efficiency
- Measurable savings and cost evasion in software license purchases and maintenance costs



About the Author



Siva R

Lead – Client Operations and Services, Infosys BPO Limited

Siva is a practicing professional in the field of strategic sourcing of IT commodities and services. He has 22 years' experience in the industry and currently manages the IT category council in Infosys. Siva leads a team of experts in the US for managing the operations and services for a Telecom giant.

About Infosys

Infosys is a global leader in consulting, technology and outsourcing solutions. We enable clients, in more than 50 countries, to stay a step ahead of emerging business trends and outperform the competition. We help them transform and thrive in a changing world by co-creating breakthrough solutions that combine strategic insights and execution excellence. Visit www.infosys.com to see how Infosys (NYSE: INFY), with US\$8.25 billion in annual revenues and 165,000+ employees, is Building Tomorrow's Enterprise® today.

Infosys BPO, the business process management subsidiary of Infosys, provides a broad range of enterprise and industry-specific services. We deliver transformational benefits to clients through our proprietary Process Progression Model™ (PPM). These benefits include cost reduction, ongoing productivity improvements and process reengineering.



For more information, contact infosysbpo@infosys.com

www.infosysbpo.com

© 2014 Infosys Limited, Bangalore, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.