

# Guidelines on Software Asset Management

---

Version 0.3

## Contents

1 Introduction .....	- 2 -
1.1 Issues and Challenges .....	- 2 -
1.2 Need .....	- 3 -
2 Software Asset Management (SAM) .....	- 3 -
2.1 Key Procedures for Implementation .....	- 4 -
2.2 Governance Structure .....	- 5 -
2.3 Implementation Details .....	- 7 -
2.4 Strategic Control .....	- 9 -
2.5 Security .....	- 11 -
3 Audit and Compliance .....	- 11 -
4 Maturity of SAM Policy .....	- 12 -
5 SAM Tools .....	- 14 -
6 Benefits of SAM .....	- 16 -
7 Acknowledgements .....	- 18 -
8 Annexure A: International Standard on SAM .....	- 19 -
9 Annexure B: SAM – Indian eGovernance Examples .....	- 20 -

## 1 Introduction

The growth of ICT and in particular web based technologies has transformed the interaction between the Government and its service seekers. Today, Governments worldwide want to use the potency of ICT to deliver end to end services right at the citizen doorstep, anytime and at minimum cost. ICT is increasingly being seen as the only way to improve governance. With the increase in accessibility to Internet and mobile technology, citizens themselves are expecting more and more online information and services from governments.

The National e-Governance Plan (NeGP) was approved by the Government of India in May, 2006 in order to promote e-Governance on a massive scale. Until the formulation of this plan, e-Governance was a subject purely driven by individual effort rather than a national vision. The National e-Governance Plan is basically a shift in the approach and methodology followed by the Departments to implement ICT initiatives prior to its formulation. Lessons and experiences from past successful and failed ICT initiatives both national and international have been blended in the new NeGP approach and methodology.

The National e-Governance Plan seeks to lay the foundation and provide the impetus for long-term growth of e-Governance within the country. The plan seeks to create the right governance and institutional mechanisms, to set up the core infrastructure and policies and to implement a number of Central, State and Integrated Mission Mode Projects, with well defined service levels, to create a citizen-centric and business-centric environment for governance. Implementation of e-Governance projects is a highly complex process requiring provisioning of hardware & software, networking, change management and capacity building. This is a perfect scenario for the deployment of a robust software asset management policy.

Software is an intangible asset protected by copyright and contract law. Due to its intangible nature, software presents unique challenges in terms of asset management. This challenge is further compounded when it comes to the management of software assets for an entity as large and complex as the Government of India.

### 1.1 Issues and Challenges

Information Technology has fundamentally changed the way we communicate, deliver services, access/store/transmit information, conduct businesses and undertake daily online transactions. As the Government undertakes critical and widespread e-Governance projects and transacts with citizens and entities, through computers and network, powered by software applications, managing IT assets has become a challenging and important task.

Some key trends/challenges being faced by organizations today are:

- Management of all strategic IT assets
  - Licenses
  - Upgrades

- Documentation
- Software versions
- More client machines (PC/Laptops) and Mobile Devices connected to unsecured networks.
- Increasing frequency of virus and security attacks.
- Increasing frequency of client security patch releases.
- Wider usage of open source and licensed software with differing licensing agreements.
- Many License agreements require mandatory periodic independent audits

An effective Software Asset Management (SAM) framework will ensure that the Department is ready to deal with the challenges posed above and at the same time complies with the regulatory, legal, IPR and security requirements of the Software being used.

## 1.2 Need

In order to establish a Software Asset Management Framework, a need has been felt to establish a Guideline for the Departments executing e-Governance projects which can be used to institutionalize policies and procedures specific to the Departments while following the basic principles of SAM. The purpose of this document is to provide practical assistance to Government of India departments in maintaining a framework for the management of software licenses and associated media. Implementation of the guidelines will provide assurance to departments and the Government that:

- a clear management policy for projects for open source, licensed and customized software is established.
- project based software assets are integrated with existing software assets in the department.
- a clear software asset ownership policy covering the entire asset life-cycle of the assets and project is established.
- to prevent use of illegal software.
- to comply with software license conditions is adequately monitored.
- there are the appropriate number of licenses for each item of software in use.
- there are effective controls in place for the physical security of software media.

Recognizing that various Departments differ in their goals, operations and their composition, the guiding principles are designed to serve as the common denominator allowing Departments sufficient latitude in creating Department specific plans while providing a unifying platform for all Government asset management efforts.

## 2 Software Asset Management (SAM)

According to the Information Technology Infrastructure Library (ITIL), SAM is defined as “...all of the infrastructure and processes necessary for the effective management, control and protection of the software assets...throughout all stages of their lifecycle.”

SAM is a business practice designed to reduce information technology costs, limit risks related to the ownership and use of software, and increase IT and end-user efficiencies. ISO 19770 Standard is the international standard on Software Asset Management (SAM) – Annexure 1.

## 2.1 Key Procedures for Implementation

2.1.1 There are a number of key issues that guide the initial planning and implementation of a SAM framework that should be addressed before developing an implementation plan. These include, but are not limited to:

- Gaining senior management support
- An assessment of the risks involved in not implementing a framework: over-licensing, under-licensing, increased expenditure, security breaches, software compatibility issues, lost time and lack of technical support and product upgrades.
- An assessment of benefits of implementing a framework: savings through purchasing only what is needed when it is needed, employees being able to work more efficiently, assists with the compilation of an accurate budget, ability to manage and monitor usage to link with ICT planning.
- The development of a business case to demonstrate the effectiveness of the framework
- Consideration of what functions may be centralized: for example, license management, procurement and software asset registers.
- Long term management: including continuous improvement, upgrades, compliance and audits

2.1.2 Software needs to be controlled throughout its entire lifecycle, from the initial request to de-installation from a machine. The Lifecycle diagram below (fig. 1) outlines all of the key procedures that should be established to support and maintain a successful framework.

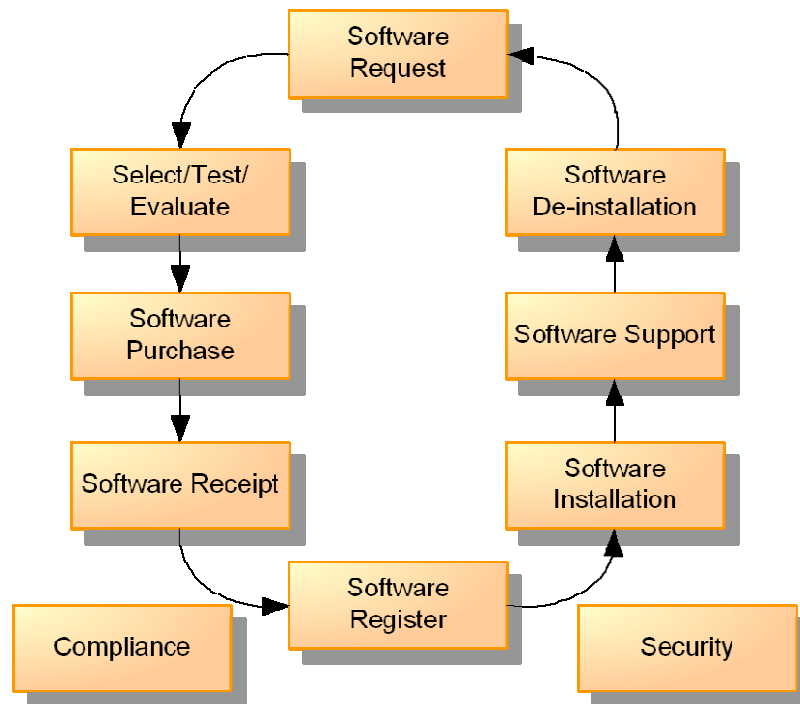


Figure 1

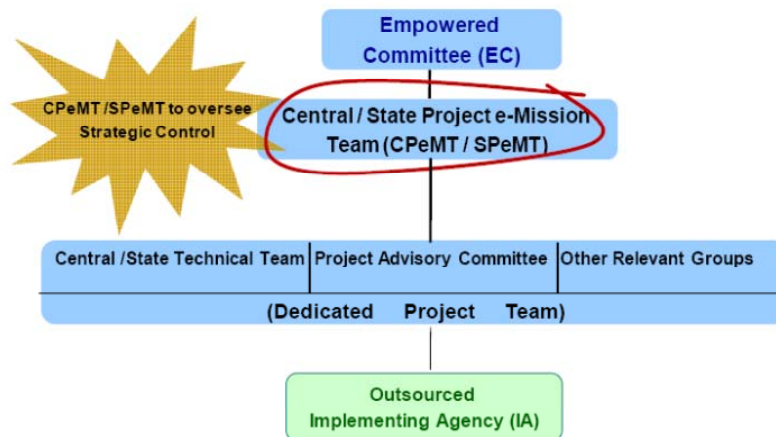
## 2.2 Governance Structure

2.2.1 NeGP comprises of core and support infrastructure components and at present 27 Mission Mode Projects (MMPs). In order to manage the complexities involved in the implementation of the Mission Mode Projects, expert resources in the areas of Technology, Project Management, Change Management, Cyber Security and Legal need to be available on full time basis at the individual Departments/ Line Ministries of the Government of India.

2.2.2 Mission Mode Projects are owned and spearheaded by various Line Ministries/ Departments. The Line Ministries/ departments are solely responsible for all the decisions connected with their MMP from conceptualization, design, development, implementation to operations and maintenance phase.

2.2.3 Governance Structure depicted in Figure 2 is suggested in the Operational Guidelines<sup>1</sup> issued by Dept. of IT, GoI. This section describes various elements of Governance Structure which have to be leveraged for retaining the Strategic Control within the Line Ministry/Department. Further details on Governance Structure including Roles and Responsibilities are provided in Operational Guidelines. The suggested Governance Structure is mentioned below.

<sup>1</sup> The Guidelines are available at [http://www.mit.gov.in/sites/upload\\_files/dit/files/Guidelines\\_Operational\\_Model\\_V42\\_231210.pdf](http://www.mit.gov.in/sites/upload_files/dit/files/Guidelines_Operational_Model_V42_231210.pdf)



**Figure 2:** The Governance Structure as per the Government of India Operational Guidelines

**Empowered Committee (EC)**, with Secretary of the Line Ministry as its Chairman, shall be responsible for overall guidance, for deciding policy level matters and to act as final body for approving all deliverables relating to the Programme and also take up responsibility of monitoring of implementation of Software Asset Management Guidelines.

**Central Project e-Mission Team (CPeMT)** is headed by a senior domain representative from the Line Ministry as the Project Mission Leader. The Central Project e-Mission Team (CPeMT) has the overall responsibility of project design, development, supervision, guidance, evaluation and monitoring of the implementation, business process re-engineering implementation of an e-Governance project and shall be responsible for exercising Strategic Control. To effectively manage various activities of the project development and implementation, various subgroups could be formed under CPeMT to support its activities. The two key subgroups are Central Technical Team (CTT) and Process Advisory Committee (PAC).

- **Central Technical Team (CTT):** The responsibility of CTT inter alia includes providing technical leadership and **ensuring** Strategic Control over the project and management of all Strategic Assets. CTT shall be responsible for implementation of SAM Guidelines.
- **Process Advisory Committee (PAC):** PAC is responsible for providing process level inputs and functional requirements.

Head of Dedicated Project Team/ Chairman of CTT to be overall responsible for SAM

The Dedicated Project Team will assist the Mission Leaders of the MMP's and other IT initiatives by providing strategic direction and leadership to ensure the project are implemented successfully, the outcomes envisaged from the project are realized and ensure implementation of SAM Guidelines as per the details given below in Para 2.3.3.

## 2.3 Implementation Details

2.3.1 The implementation of SAM involves four stages:

- Initiation
- Assessment
- Prioritization
- Implementation

Initiation:

- Commitment and support of senior management
- Formulation & formalizing the SAM strategy
- Defining policies & initial procedures

Assessment:

- Manual inventory of software
- Automatic inventory using software inventory tools
- Mapping of licenses

Prioritization:

- IT strategy
- IT budget
- Usage pattern
- Legal/Regulatory considerations

Implementation:

- Implement technology
- Implement people processes
- Implement processes and procedures

2.3.2 A flowchart to practically implement the four stages:



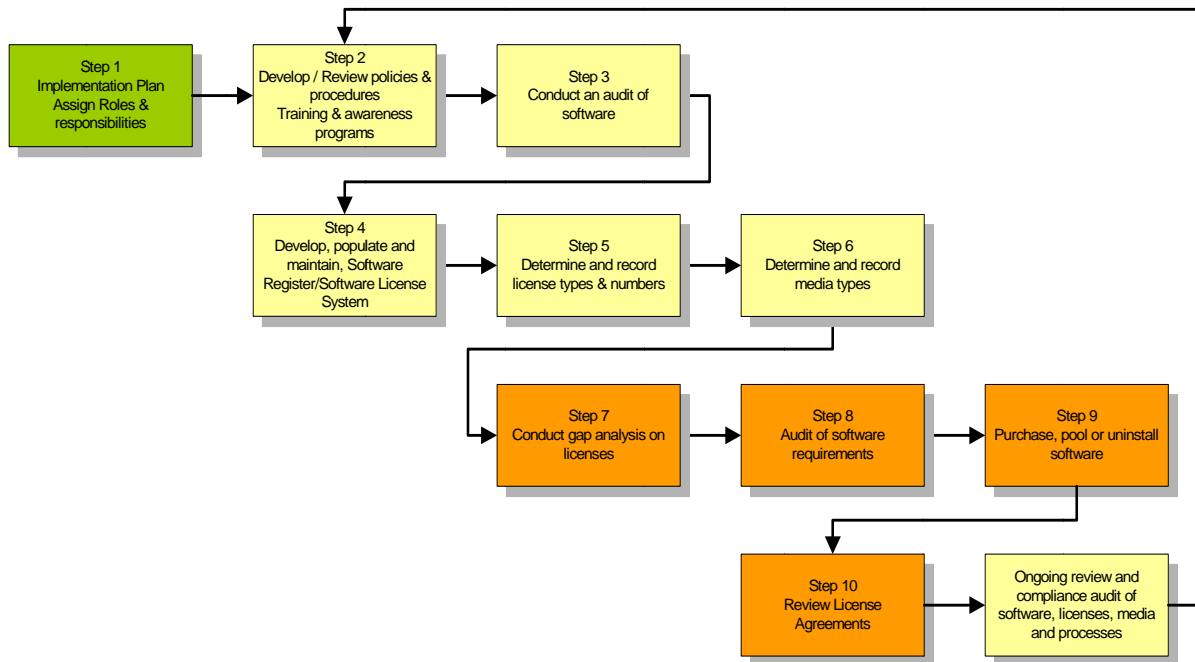


Figure 3

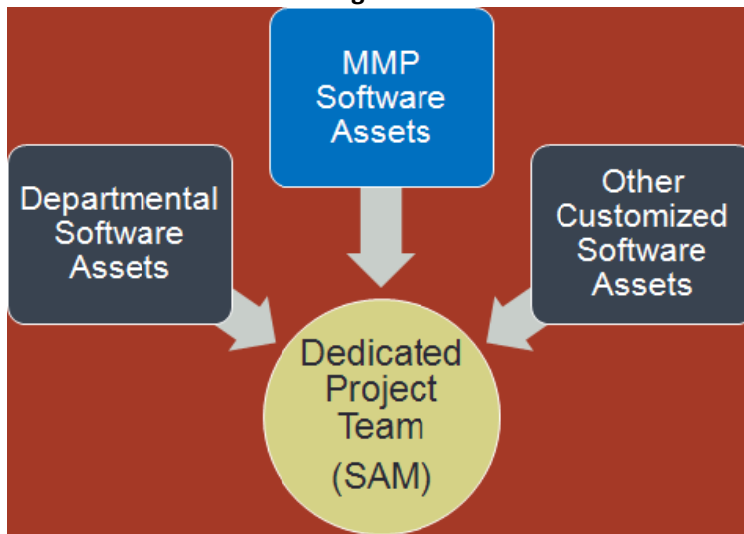


Figure 4

### 2.3.3 Roles and Responsibilities of Dedicated Project Team for SAM:

#### Establishing Organization Policies

- Establish a SAM cell within the Dedicated Project Team
- Establish software use, copyright and personal software usage policy
- Rigorously enforce the policies

#### Designing and Implementing Procedures

- Formalize procedures installation, disposal and retirement of Software
- Formalize procedure for acquisition and transfer of licenses

- Formalize procedure for standardization of Software within MMP and Department
- Formalize procedure for Storage and Disaster protection
- Ensure adherence to Guidelines for Strategic Control for customized applications/software

#### Managing and Maintaining Records

- Software inventory management system
- Hardware Inventory management system
- License Inventory management system
- Asset documentation management system
- Management Systems for the assets of Customized software as detailed in the Strategic Control guidelines

#### Ongoing Management and Review

- Manage the versions and related documentation of Application Software
- Continuous monitoring for adherence with SAM policy
- Periodic review and update of procedures
- Periodic review of Inventory systems
- Continual improvement of the SAM framework

## 2.4 Strategic Control

Information Technology (IT) has emerged as a key driver in improving the efficiency in the Government Processes thereby facilitating higher levels of service delivery to the citizens and other stakeholders. Additionally, it is also improving the effectiveness, accountability and transparency of the Government processes. To expedite the implementation of IT projects especially in the area of e-Governance, participation of Industry both as partner and vendor has become essential. This has resulted into a significant increase in the role and responsibilities of the Industry and Private Sector in such projects. Although outsourcing to Industry has increased the bandwidth for implementation of the projects, it has also necessitated the need of retaining Strategic Control<sup>2</sup> within the Line Ministries/Departments over the project life cycle, its deliverables and outcome.

Implementation of SAM facilitates the Line Ministry/department to retain the Strategic Control within government by enabling taking over the management of all the customized software assets created under the project and also by taking over all the licensed software procured by the outsourced agency for the implementation of the project. It also further defines the four key factors i.e People, Policies, Processes, and Infrastructure which are essential in maintaining proper controls in an outsourced project.

---

<sup>2</sup> Guidelines for Strategic Control in Outsourced Projects are available at [http://www.mit.gov.in/sites/upload\\_files/dit/files/Guidelines\\_setting\\_Dedicated\\_Project\\_Teams\\_251110.pdf](http://www.mit.gov.in/sites/upload_files/dit/files/Guidelines_setting_Dedicated_Project_Teams_251110.pdf)

The 4 key factors which are essential in maintaining proper controls in an outsourced operation are – People, Policies, Processes, and Infrastructure. These match with the 4 key components that the paradigm of SAM rests on.



**Figure 5**

The key elements of each of these components are further elaborated below:

#### **2.4.1 People**

- a. Organization structure
- b. Employee Contracts and non-disclosure agreements with vendor(s)
- c. Background check and screening of employees (presently being done in case of Defense contracts)
- d. Induction and regular training programmes to orient staff regarding Security measures.
- e. Supervisory control by Departmental/ Government staff.
- f. Attracting and retention of the right skills - To effectively manage the outsourced activities it is important to maintain the core skills internally.
  - i. One way of retaining / building skills internally, retaining interest of staff and helping to build a common culture is through rotation of staff.
  - ii. Strong motivators to attract talent:
    - a. Challenging work in public sector
    - b. Ability to develop new skills both on the job and through trainings.
  - iii. Reward and recognition programs are important.
  - iv. Two different pay scales for internal and external staff are considered to be a problem. The salary differential should not be more than 30%.

#### **2.4.2 Policies**

- a. Documented organization policies
- b. Role based authorities and access
- c. Data classification (critical, manageable & commodity)
- d. Role classification
- e. Decision making controls in line with the governance model.
- f. Design for proper security and controls
- g. Integration of security with delivery life cycle. Security policy should be comprehensive and should cover access privileges, encryption policies, vetting procedures (as indicated earlier), audit trails, network security etc.

- h. Emphasis on approved security frameworks and policies
- i. Strict penalties for non-compliance.
- j. If possible divide the job region wise to multiple vendors. This will maintain competitive environment and also back-up in case of any failure.

#### **2.4.3 Processes**

- a. Application specific access and security controls.
- b. Define core/non-core processes for management controls.
- c. Comprehensive logs of all operations / transactions and regular review
- d. Controls on database, network, OS etc
- e. Intellectual property protection
- f. Business continuity planning
- g. Regulatory compliance
- h. Periodic Audits

#### **2.4.4 Infrastructure**

- a. Define enterprise security standards.
- b. Physical security and access controls
- c. Network security, firewalls, perimeter, and endpoint defenses.
- d. Monitoring and compliance of security standards.
- e. Detailed risk assessment.
- f. Regular security audits.

## **2.5 Security**

Security features can help prevent the theft or the unauthorized use of a system.

Security features generally available with SAM include:

- Passwords, power-on passwords, set-up passwords
- Smart cards or biometrics technology for access protection
- Security locks, which can be activated remotely
- Central and remote activation and deactivation of the system, its components (diskette drive, hard disk, ports and so on) or both
- Disabling of interfaces (serial, parallel, Universal Serial Bus [USB]) locally and remotely.

## **3 Audit and Compliance**

An audit of the agency's deployed software should be undertaken to ascertain what software is installed on its computer networks and devices. The initial audit should provide an accurate report of the quantities of software products deployed within the agency.

Once collected the key information should then be collated into a Software Asset Register (SAR) to assist in matching software in use with agency license details.

### **3.1 Audit**

At its simplest it involves the following:

- Identification of Software Assets
- Verifying the Software Assets including licenses, usage, and rights
- Identifying gaps that may exist between what exists on the installations, and the licenses possessed, and the rights of usage
- Taking action to close any gaps
- Recording the results in a centralized location with Proof of Purchase records
- Compliance to notified standards

### **3.2 Compliance**

An effective SAM framework would ensure:

- Business practices are in line with applicable laws
- Adequate safeguards have been taken to cover the legal risks at appropriate software lifecycle stages (Contracting, Procurement)
- Policies and procedures are in tune with legal requirements
- Personnel are aware of the legal risks posed by unauthorized/pirated software
- Regular monitoring is done to assess compliance

Benefits of Compliance:

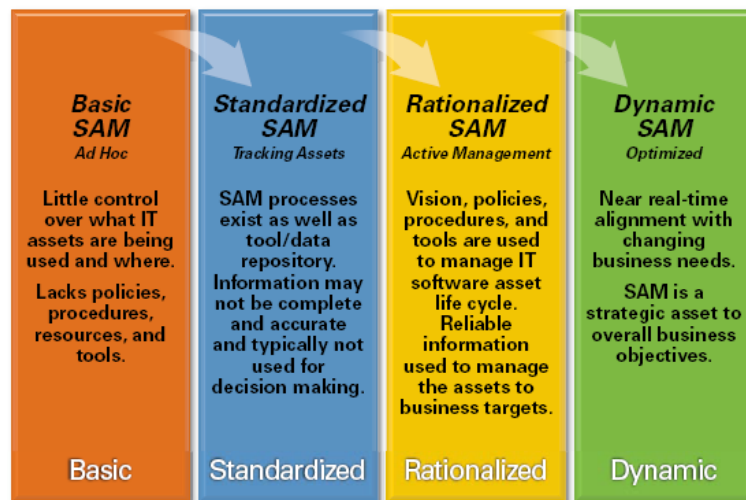
- Reduced risk and liability for intentional or unintentional copyright infringements
- Better software license management with reduced incidence of over or under licensing

## **4 Maturity of SAM Policy**

The SAM Optimization Model provides a framework to evaluate the maturity of SAM processes, policies, and tools. The model maps to the ISO/IEC SAM standard 19770-1 and is based on the Infrastructure Optimization (IO) model: in order to achieve each level of IO, there needs to be in place a corresponding level of SAM optimization to support it. Ultimately, it is critical for all organizations/governments to know what IT assets (software and hardware) they own and where they exist. Without this knowledge an organization cannot effectively address challenges such as optimization, server consolidation, virtualization, information security, business continuity, and configuration management.

4.1 The corresponding levels of SAM maturity that enable overall IO maturity are shown below:

### SAM Optimization Model



Source: Microsoft Corporation

Figure 6

4.2 Key component questions which are part of the SAM Optimization Model, and designed to measure an organization's/government's overall level of SAM maturity:

1. *SAM Throughout the Organization* – Generally, organizations/governments that have made an effort related to SAM appear to have started with this first competency by assigning SAM roles and responsibilities throughout the organization.  
Well documented SAM policies and procedures – Organizations generally understand the need to have formally documented SAM processes to be successful in running a SAM program. Only those SAM programs that are embraced by upper management are successful.
2. *SAM Self-Improvement Plan* – Organizations that have enough cumulative maturity to be at the Standardized or Rationalized level overall may benefit from developing a formalized strategy and SAM improvement plan.
3. *Hardware and Software Inventory* – This is a key indicator of overall maturity.
4. *Accuracy of Inventory* – Accuracy of inventory is a good predictor of overall maturity.
5. *License Entitlement Records* – Some organizations/governments may have more complete entitlement records than anticipated because the license entitlement inventory is managed as a separate process (e.g. by procurement), even if IT operations processes are not implemented in a mature way.
6. *Periodic Self-Evaluation* – Those organizations/governments that collect and maintain inventory records for deployment and entitlement are likely to perform periodic reconciliations of such records.
7. *Operations Management Records and Interfaces* – Lockdown of user PCs – If PCs in their environment are not locked down to prevent downloading unauthorized software, it can expose an organization to issues related to license noncompliance.

Centralized Software Distribution – Lack of this could lead to installations that cannot be tracked and supported and is an indication of poor SAM practices and maturity.

8. *Acquisition Process* – Disconnects between the acquisition process and the deployment process are a root cause of issues when new assets are added to the operational environment.
9. *Deployment Process* – The key risk that most organizations face is in the interfaces between the acquisition and deployment processes. The root cause of most license compliance issues is the “disconnect” between IT administrators who deploy software, procurement offices, and legal contract administrators who acquire software. IT, legal, and procurement organizations may be implementing each process effectively on their own, but issues result if these key stakeholders for SAM do not have both structured and open communication processes.
10. *Retirement Process* – Compared with other key processes in the IT asset life cycle, retirement management is often literally left until the end and then often forgotten or ignored. Organizations/governments that have mature processes and procedures related to other aspects of the software life cycle may benefit further by implementing effective retirement processes.

## 5 SAM Tools

Finding the right software licensing systems and tools can be a big challenge primarily owing to the immaturity of the software asset management tool and license management software solution market and the types of system available either of the database (simple) or workflow-database (advanced) variety, and compatibility with existing network and software/hardware infrastructure of the organization. In such a scenario, it is important to have a detailed categorization of the SAM tools available.

SAM tools concentrate on five key functions:

- inventory and asset management
- security
- system settings configuration, deployment and software updating
- fault and performance management
- integration with enterprise management tools

Various categories of tools which could be used are given in the table below (Figure 7):

Tool Category	Features Offered
Asset Inventory Tools	<ul style="list-style-type: none"> <li>• Allows management of inventory of software assets and licenses</li> <li>• Offers simple tools (Excel) to complex systems (GASP)</li> </ul>
Asset Discovery Tools	<ul style="list-style-type: none"> <li>• Identifies hardware and software installed in the company</li> <li>• Checks software on all platforms</li> <li>• Cannot work on stand-alone PCs</li> <li>• Does not work for new applications/internally developed applications</li> <li>• One server application may be used by many users, since the tools looks at application instances</li> </ul>
Metering Tools	<ul style="list-style-type: none"> <li>• Checks use of software on workstations</li> <li>• Can be Passive (check usage) or Active (check licenses)</li> <li>• Sends exception reports (exceeding license limits)</li> <li>• Cannot be used for stand-alone PCs</li> </ul>
License Management Tools	<ul style="list-style-type: none"> <li>• Allows for management of license information</li> <li>• Periodically determines a need for each type of software license used</li> <li>• Traces the license requests with license's effective use</li> <li>• Identifies unused licenses</li> </ul>
Contract Management Tools	<ul style="list-style-type: none"> <li>• Manages all the issues related to software purchase contracts and their installation</li> <li>• Checks for terms of contract, their possible automatic renewal or expiry dates</li> </ul>
Deployment Management Tools	<ul style="list-style-type: none"> <li>• Monitors software during the deployment stage</li> <li>• Allows installation with related authorizations</li> </ul>
Security Tools	<ul style="list-style-type: none"> <li>• Prevents the installation of unauthorized software</li> <li>• Prevents changes in the released and authorized configurations</li> </ul>
Procurement Tools	<ul style="list-style-type: none"> <li>• Allows for purchase of new licenses</li> </ul>
Vendor License Management Technology	<ul style="list-style-type: none"> <li>• Uses Licensing keys</li> <li>• Makes use of hardware dongles</li> <li>• Allows for online license management</li> <li>• Performs Software Metering</li> </ul>

Figure 7



## 6 Benefits of SAM

6.1 A holistic consideration of SAM involves managing and improving all aspects of software assets across most operational and organization components of the company. This big-picture view not only helps companies build a more strategic and integrated approach to software licenses; it also helps increase the number of benefits associated with effective management and their potential impact. Among those benefits:

### **Cost control:**

- Less legal- and compliance-related expenses, including software audits.
- Better management of operational costs related to maintaining license compliance. For example, securing better software licensing contracts — in which deployment and technical architecture are clearly outlined and understood — helps companies to negotiate more favorable deals with software vendors, thereby lowering overall costs of their software procurement. Cost avoidance is achieved by rationalizing the software portfolio to reduce redundant, overlapping or no-longer-necessary software licenses.

### **Reduction of risks:**

- Contractual risk – Effective SAM helps to optimize clients’ negotiating position with their vendors, outsourcers and potential merger & acquisition partners. Companies armed with complete and insightful information will be better able to prevent third-party providers from inserting increased risk premiums into their offers.
- Reputational risk – Clients may face public disclosure of under-licensing, which could lead to significant adverse media coverage and penalties.
- Financial and budgetary risk – While settlements of vendor audits are normally confidential, vendor audit activity has been increasing. There have been settlements in many cases in multiples of millions of Euros per vendor for unlicensed application. A recent Gartner report indicates that more than 50% of their clients polled have been audited by at least one software vendor in the last 12 months.
- Information security risk – Inadequately licensed software introduces the possibility that clients may have deployed counterfeit and potentially unauthorized software. There is a risk that such software may include malicious code and be operating at sub-standard levels.

### **Optimization of current assets and process:**

- Enables license overpayment recovery.
- Facilitates preparations for mergers and acquisitions.
- Helps make vendor audits more time- and resource-efficient and delivers stronger negotiating position through better management of license-related contracts.
- Helps IT leaders make better decisions through the use of better information.
- Increased confidence by both internal and external stakeholders.
- Promotes more efficient IT systems; less time and money spent toward compliance, and more into making IT a more effective and strategic contributor to overall company goals and objectives.

6.2 An often neglected but important area of SAM is Software Retirement Management. Software Retirement Management benefits include:

- Cost optimization (e.g., reuse of retired software from retired PCs)
- Accurate records (keep hardware and software inventories accurate; enable reconciliation between the financial fixed-asset ledger and the actual IT environment)
- Social responsibility (many organizations/governments donate old hardware and software and help to ensure “green” recycling)
- Security and risk management (e.g., hard-disk wipe and other initiatives to protect customer and corporate private and confidential information)
- License compliance risk mitigation (e.g., if legacy PCs and servers are not appropriately retired, the company is required, per the license product use rights, to maintain licenses for these items)

## 7 Acknowledgements

1. Queensland Government – Software Asset Management (SAM) Guideline
2. Queensland Government - Best Practice Guide for Third Party Software License Management
3. KPMG – SAM: A Key to Infrastructure Optimization
4. Business Software Alliance – Guide to Software Asset Management
5. Business Software Alliance – Government Guide to Software Asset Management
6. Business Software Alliance - The Business Benefits of Software Asset Management
7. Business Software Alliance – Standards Based Software Asset Management Principles
8. Data Security Council of India - Asset Management Book
9. Government of India - Guidelines for Strategic Control in Outsourced Projects
10. Government of India – Guidelines for Setting up Dedicated Project Team
11. Government of India – NeGP Guidelines for Operational Model for Implementation of Mission Mode Projects by the Line Ministries/State Departments
12. Ernst & Young – Effective Software Asset Management: How to Reap its Benefits
13. <http://www.indiatechonline.com/bsa---karnataka-government-partnership-251.php>
14. <http://www.bsa.org/country/News%20and%20Events/News%20Archives/hi/2010/hi-10132010-ficci.aspx>
15. <http://www.newkerala.com/news/world/fullnews-128649.html>
16. <http://www.iso19770.com/>
17. [http://www.foursquareinnovations.co.uk/software\\_asset\\_management.html](http://www.foursquareinnovations.co.uk/software_asset_management.html)

## 8 Annexure A: International Standard on SAM

The development of the International Standard on SAM is a global project led by Swedish Standards Institute (SIS).

The International Standard on SAM is unique as it combines process descriptions and software adaptations without the two parts being dependent on each other. When performing inventories of installed software, everything is scanned and the result is often difficult to understand due to the volume and complexity of information reported. The definitions in part two of the standard will enable identification to be simpler therefore making the inventory process more efficient and effective.

8.1 ISO 19770 Standard is the international standard on SAM. It is a two part standard, covering:

- Business issues (ISO 19770-1): was developed to enable an organization to prove that it is performing SAM to a standard sufficient to satisfy corporate governance requirements and ensure effective support for IT service management overall. It covers the processes and procedures for SAM planning, inventory control and software lifecycle management
- Technical issues (ISO 19770-2): technical specifications and metrics (under development)

IS Governance framework entails SAM and is based on the following standards:

- ISO 27001 Information Security Management System
- BS 15000 IT service management

These standards mandate compliance with regulatory requirements for restricting copying of software in organizations.

8.2 ISO 19770 has six main sections:

- Control environment, which deals with processes, procedures, roles and responsibilities.
- Planning and implementation, which deals with resource required, reporting structure, measurement and verification.
- Inventory, which deals with selection and confirmation of assets, monitoring of existence, usage and storage.
- Verification and compliance, which deals with processes to identify and match inventory to licenses.
- Operations management, which deals with documentary evidence of implementation, and management of relationships with vendors.
- Lifecycle, which deals with software lifecycle management.

## 9 Annexure B: SAM – Indian eGovernance Examples

### 9.1 Karnataka taps BSA to beef up software management in government

The Center of E-Governance of the Karnataka Government has joined hands with the India operation of the Business Software Alliance (BSA) to bring the benefits of Software Asset Management (SAM) to state-based Public Sector Undertakings and government departments. SAM, an ISO (2006) standard, enables companies and organizations to efficiently and effectively manage and track their software licenses as valuable company assets throughout its life cycle of procurement, deployment, usage, maintenance and retirement, enabling cost savings, risk management and operational efficiencies. Karnataka has already engaged with BSA to introduce SAM to small and medium enterprises in the state and the new partnership will help spread the culture within public undertakings engaged in key sectors including transport and energy, explains D.S. Ravindran, CEO of Karnataka government's Centre for e-Governance. The state has been judged number one in e-readiness among all Indian states and its total annual spending on IT is around Rs 3 billion, Dr. Ravindran added.

### 9.2 BSA-FICCI WRC Recognizes SMEs on Software Asset Management Leadership in Maharashtra, supported by Government of Maharashtra

Business Software Alliance (BSA) in partnership with FICCI (Western Regional Council) awarded the BSA Certificate of Recognition to 26 companies under the "Leadership in Software Asset Management" Program as part of the "Progressive Maharashtra" initiative aimed towards building sustainable competitive advantage in the state supported by the Government of Maharashtra. The "Leadership in Software Asset Management" Program aimed at promoting the value of software licenses as organizational assets, importance of IT Governance and Intellectual Property Rights in Software, to enable small and medium enterprises in the state to become IT competitive and mature by adopting world-wide best practices in implementing IT policies and procedures through the ISO recognized standard of Software Asset Management (SAM).

As part of the SAM Leadership Program, more than 500 SME companies were sent education and awareness material on SAM and related areas. Additionally, a total of 45 SMEs across industry sectors in Maharashtra participated in the Software Asset Management Certification Program organized and executed by BSA, supported by FICCI (WRC), which comprised of educational and awareness workshops and voluntary SAM review assessments for the SMEs which came forward to evaluate their organizational maturity of their IT environments, policies and procedures and assessment of their software licenses. Twenty six companies were finally awarded "Certificates of Recognition" for successfully fulfilling all the elements of the program.

### **9.3 BSA launches software asset management programme in Andhra**

Hyderabad, Jan 20, 2011: After success in Karnataka and Maharashtra, Business Software Alliance (BSA) announced the launch of its education and certification programme - leadership in Software Asset Management (SAM) - in Andhra Pradesh.

To be supported by the state government, the programme is aimed at improving corporate governance through cost cutting and improved efficiency among small and medium enterprises (SMEs).

Keshav S. Dhakad, chair, BSA India Committee, told reporters that awareness would be created among SMEs on the benefits of SAM, an ISO 19770:1 standard, which promotes the value of managing software licenses as assets within companies and organizations.

"Through this programme, BSA aims to enable Andhra Pradesh to become a leading state in promoting SAM-led strong corporate governance standards in the field of IT within the local companies, driving cost efficiencies, better risk management and achieving high levels of IT maturity and improve security," he said.

The participation and recognition under the programme would help SMEs control costs, enhance productivity, network security and fulfill compliance obligations. "It would help participating companies to enhance their brand reputation and attract international clients and investors by showcasing their improved organization management, through the certification under the programme," Dhakad said.

Ravi Prasada Rao, joint director, e-governance in Andhra's information and communication technology department, said 1,000 to 1,200 SMEs in and around Hyderabad could immensely benefit from this four-month long certification programme.

The state government proposes to empanel SAM-certified SMEs for awarding the government works in e-governance.