IAITAM ACE

KICKIN' ASSETS
SINCE 2002

Software Audit Playbook

Anugrah Shukla

NASHVILLE, TN
MAY 9TH - 11TH

Software Audit Playbook

Anugrah Shukla
Software Asset Management Team Lead

Software Audit Playbook

Software license audits cost businesses millions of dollars every year and require a huge amount of time and effort to be spent by the customer during each audit.

Above mentioned Statement lays a solid foundation to prepare a Software Audit Playbook. This contains all the pieces and parts that will make up Organization's go-to approach for getting things done. The Playbook leads to "process workflows, standard operating procedures, and cultural values that shape a consistent response—the play"

Why do Vendors Audit?

Audits are triggered by the software vendors as a process for them to ensure your compliance with the various terms, metrics, and rules that comprise their licensing program or, more likely, programs.

License compliance has been a main revenue driver for the world's major software vendors for many years. This is especially true of the larger legacy vendors who are no longer innovating with new software, and who are now reliant on generating much of their revenue through compliance. Let's look at the top three reasons why vendors audit.

Reason 1: Audits Bring in Revenue

Reason 2: Possible Negotiation tactic

Reason 3: Encourages New Purchases

What Type of Audit Can We Expect?

When is an audit not an audit? License audits arrive in different shapes and sizes. Making sure we are aware of the type of audit we are working with

Formal Audit: A contractual audit that invokes the verifying compliance audit clause (including penalties). The audit is conducted either directly by the vendor's compliance team using third-party specialist auditing
firms, or by 'Big Four' accounting firms.

Self-Audit: A do-it-yourself audit targeted at smaller customers or related business entities. Contractual and part of the verifying compliance Claus.

True-Up Validation: A contractual obligation which, while not called an 'audit' in name, should be treated with care in the event of noncompliance being reported. Often the vendor will deploy a third party to check the true-up submission is correct.

Solution Assessment
A voluntary third-party assessment often popular with Microsoft partners. Helps with cloud readiness and migration/adoption strategies and technology product decisions. The true-up may be required for shortfalls, but penalties are not usually applied to payments.

The Vendor Audit Process

The 6 Steps of Audit:

01 | Audit Target Selection
License audits are not as random as they appear. How do the vendors select their audit targets? What can trigger an audit?

02 | Customer Notification
How should you respond when you receive an audit notification letter or email? What are the key first steps in successful audit defense?

03 | Audit Scoping & Initiation
Understand exactly what the vendor is contractually entitled to do during the audit and ensure you are prepared for what comes next.

04 | Audit Data Collection
What are the most common information gathering techniques used by vendors and how should you manage this activity?

05 | Factual Accuracy Verification & Confirmation
How should you review the data behind the draft compliance report issued by the vendor? Where can you identify any discrepancies or inaccuracies at this stage?

06 | Settlement Discussions
Understand how you can negotiate claims for non-compliance, minimizing your settlement fee.

The 6 main indicators

The most common triggers for a software license audit are:

1. Customer's Purchase level with the Vendor
2. Organizational Structure Complexity
3. Level of Organizational Changes such as M&A activities.
4. Complexity of licensing Model agreed
5. Purchase pattern that does not reflect growth
6. SAM Maturity Intelligence gathered from Account Team

Reducing the Chances of an Audit

1. Communicate your technology roadmap to the publisher and its place within it.
2. Demonstrating competent Software Asset Management
3. Making Regular Software Purchases.
4. Subscribing to support and maintenance if appropriate.
5. Being clear about why you maintain a legacy roadmap and the potential for upgrades.

Problem Statement

- Organizations do not have any Software license Audit ready strategy, if approached by any of the Vendors for Audit.
- Organizations is lacking cross functional collaboration between Business Owners, Application Owners and Licensing Experts.
- Millions of dollars can be saved if we have product level knowledge of license implementation, usage rights and consumption strategy.

Risks

If Organizations does not evaluate the complete risk of each of the licensing metric and related usage rights deployed throughout the environment, they will remain in a state of huge Financial ,Security, Legal and Corporate Branding Exposure.

•Misuse of licenses and unauthorized access resulting in increased license exposure and making Organizations Audit Unfit.

• License usage rights and deployment mis-management.

• Type of Audit we can expect- Formal Audit, Self Audit, True-up Validation and Solution Assessment.

• Reputational damage which may lead to loss of consumer trust and negative media coverage

Problem Solution

To respond effectively to an audit or review, we need the three pillars of audit defense in our company to meet our obligations and gather the needed data:
People , Process and Technology.

- Facilitating SAM ,Discovery and Metering tools co-ordination.

Instance-1 IBM ILMT deployment may support Multi Million USD on cost Avoidance and close-down the Audit exposure.
Instance-2 Restrictions on movement of VM's to Static clusters may support Multi Million USD on cost Avoidance.

- Conducting Annual Internal and Mock Audit practices by Leveraging Internal Audit teams from within Organizations.

- Documenting all licenses and Entitlements, Tracking On-premises and cloud installations, Understanding Entitlements, Developing a cloud strategy.

- To better the SwAM Maturity Level from Standardized to Rational and then move to Dynamic State, to achieve the Industry Standard ISO/IEC 19770.

Project Approach

To Design a framework on Software Audit Playbook for any Software Publishers for ready reference throughout the Organization.

Understand the gap	• The exposure each publisher Brings once deployed. • Evaluation of Mock and Internal Audit and gap closure.
Build Solution	• Collect Entitlement Data, tracking Installation. • Increasing SwAM Maturity
Reporting	• Detailed reports to stake holders • Tracking over-consumption and under-deployment.
Training	• Deliver Training to appropriate audience • Communication campaigns and strict actions.

Value to Organizations and Benefits

Preparedness

- Based on EY's finding, closing on the exposures of ~ Millions USD.
- Better Software Assets Utilization and cost savings/avoidance of millions of dollars.
- Increasing confidence that company has strong focus on Software license compliance.
- Automating license management process to speed up the audit response time.

Readiness

- Helping business units realize complete license utilization with 100% compliance confidence.
- Multi Million Dollar Cost saving opportunities.
- Rectification of over-deployment and management of under-utilized high-cost licenses.
- Confidence of Audit safety while license deployment.

Strategy

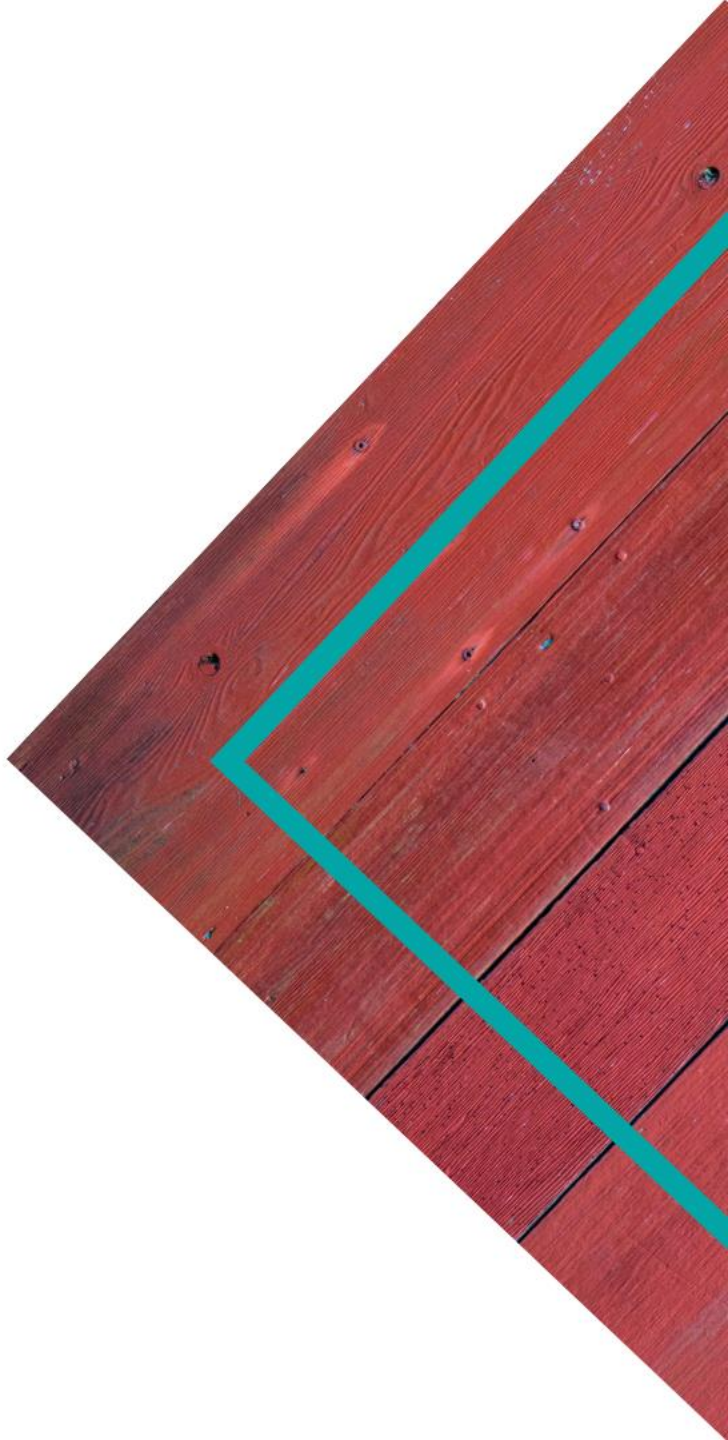
- Successful annual mock and Internal Audit reports for top level management.
- Accurate license data management vs license deployment.
- A ready to go Software Audit Playbook.

Challenges

- Level of Organizational Changes such as M&A activities and structural complexity to gather license usage data and actual deployment.
- Accurate Discovery of Software Inventory.
- Cross collaboration between different IT teams and pillars across the organization.

Learning

- Risk Assessment
- Interaction with different stakeholders
- Exposure to different tools and skillsets
- Data Management and Reporting
- Time Management
- Planning



IAITAM ACE
KICKIN'ASSETS
SINCE 2002

Project Activities

- Reports to stakeholders.
- Communication campaigns with stakeholders.
- Design and deliver training to service desk and appropriate audience.
- Implement change management.
- Creating Best Audit Practise Scenarios.
- Close associated risk with the actual deployment vs license entitlements.
- Build a solution to effectively handle critical vendor Audits.

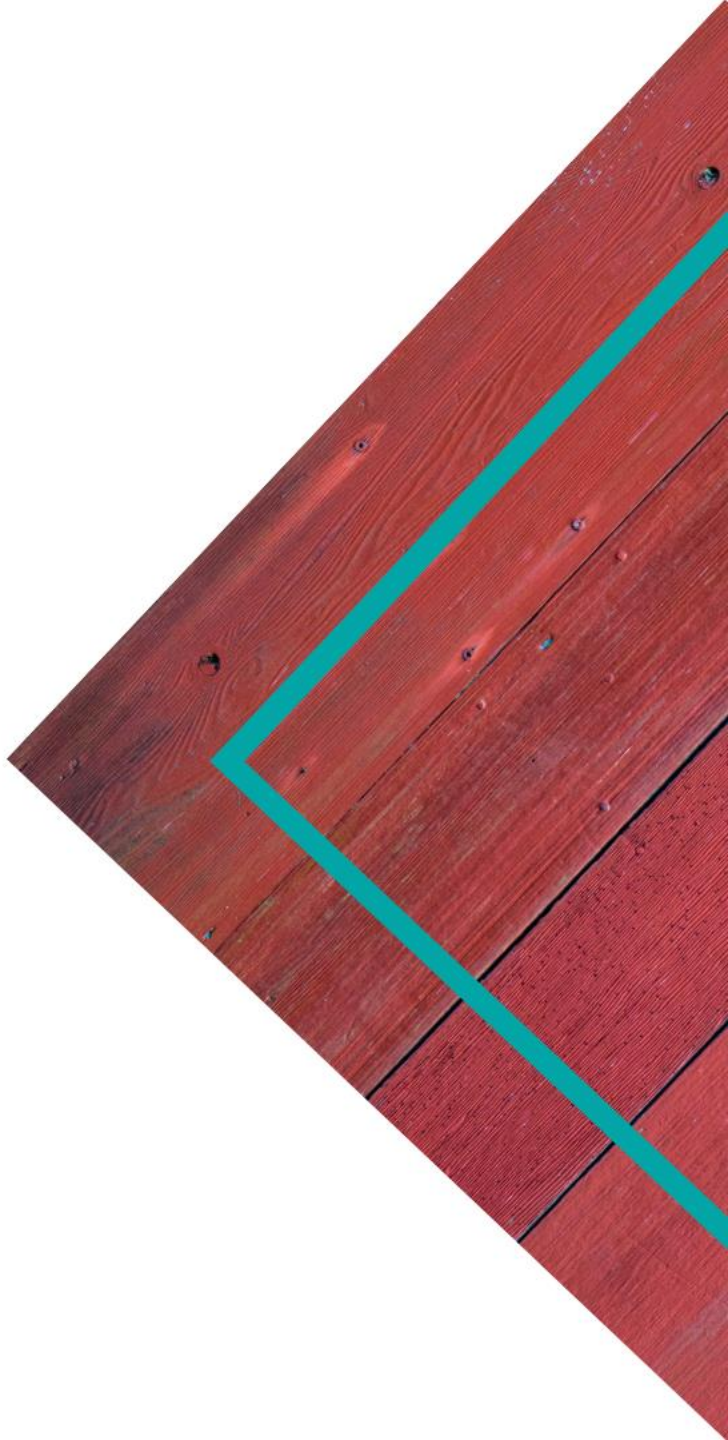
IAITAM ACE
KICKIN'ASSETS
SINCE 2002

RACI Matrix

RACI Matrix - SLB

R = Responsible A = Accountable C = Consulted I = Informed

		SAM	Internal IT	APP Owner	SAM Steer Co.	Procurement	Legal
Audit Defense							
1.1	Audit initiation communication	C	R	C	A	I,C	C
1.2	Non-disclosure agreement	C	C	I	C	I	R,A
1.3	Audit procedure and schedule	C	A	R	C	I	C
1.4	Pre-audit internal compliance assessment	A	I	C	R	C	I
1.5	Implement remediation measures	C	C	R	A		
1.6	Publisher audit scope and methodology finalization	C	A	R	C	I	I
1.7	Publisher audit coordination	C	A	R	C		
1.8	Assessment of audit findings	A	C	C	R	C	I
1.9	Discussion of audit findings with software publisher	C	A	R	C	I	
1.10	Final audit report review	A	C	C	R	C	
1.11	Final audit report discussions with the publisher	C	A	R	C	I	
1.12	Commercial negotiations	C	C	C	C	R,A	
1.13	Audit closure	I	A	R	C	I	C



IAITAM ACE
KICKIN'ASSETS
SINCE 2002

Questions
&
Answers