www.pwc.com

IIA Super Conference

Software Asset Management (SAM) Internal Audits

pwc

Agenda

- Introduction
- Software Asset Management (SAM) overview
- Potential Internal Audit Approach
- Example Risk Areas
- Summary and Questions

Jack Fulford – Biography

Mr. Fulford has over 30 years of IT experience. His experience includes software development, systems engineering, and Program Management. His most recent 8 years has been focused specifically in the IT Asset Management (ITAM) and Software Asset Management (SAM) fields. Key highlights from this time include:

- Led, leading, or supporting 8 SAM internal audit engagements for companies ranging from large technology to global property management.
- Led international team to design, develop, and execute a program to implement project planning and management for Key Account software audit engagements.
- Worked with Fortune 500 customers to leverage and develop SAM systems and processes for Oracle product discovery and measurement.
- Led 50 person, global technical analysis services and tool development team that determined customer software usage in support of software compliance audits.
- Managed and directed the SAM software development effort and requirements analysis associated with consolidating Oracle usage tools deployed in support of software audits.
- Supervised the business team responsible for implementing an integrated FFIEC compliant ITAM practice across a large Financial Services enterprise.
- Led the corporate-wide IT Asset Management (ITAM) process development and implementation team and coordinated programs between IT, Procurement, Contracts, and Accounting.
- Managed the 2007, 2008, and 2009 MS True-up initiatives for a large financial services firm and saved over $8M by tracking software utilization, applying cost reallocation, and license harvesting.

Software Asset Management Overview

What is SAM?

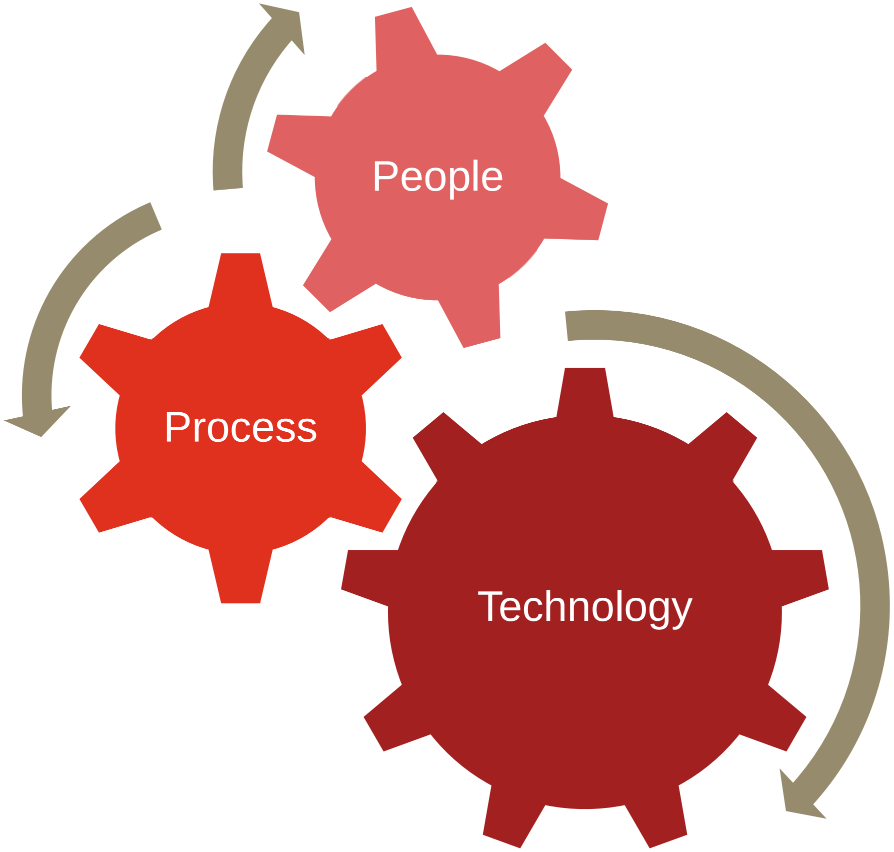
Software Asset Management (SAM)
is the practice of integrating

people,

processes, and

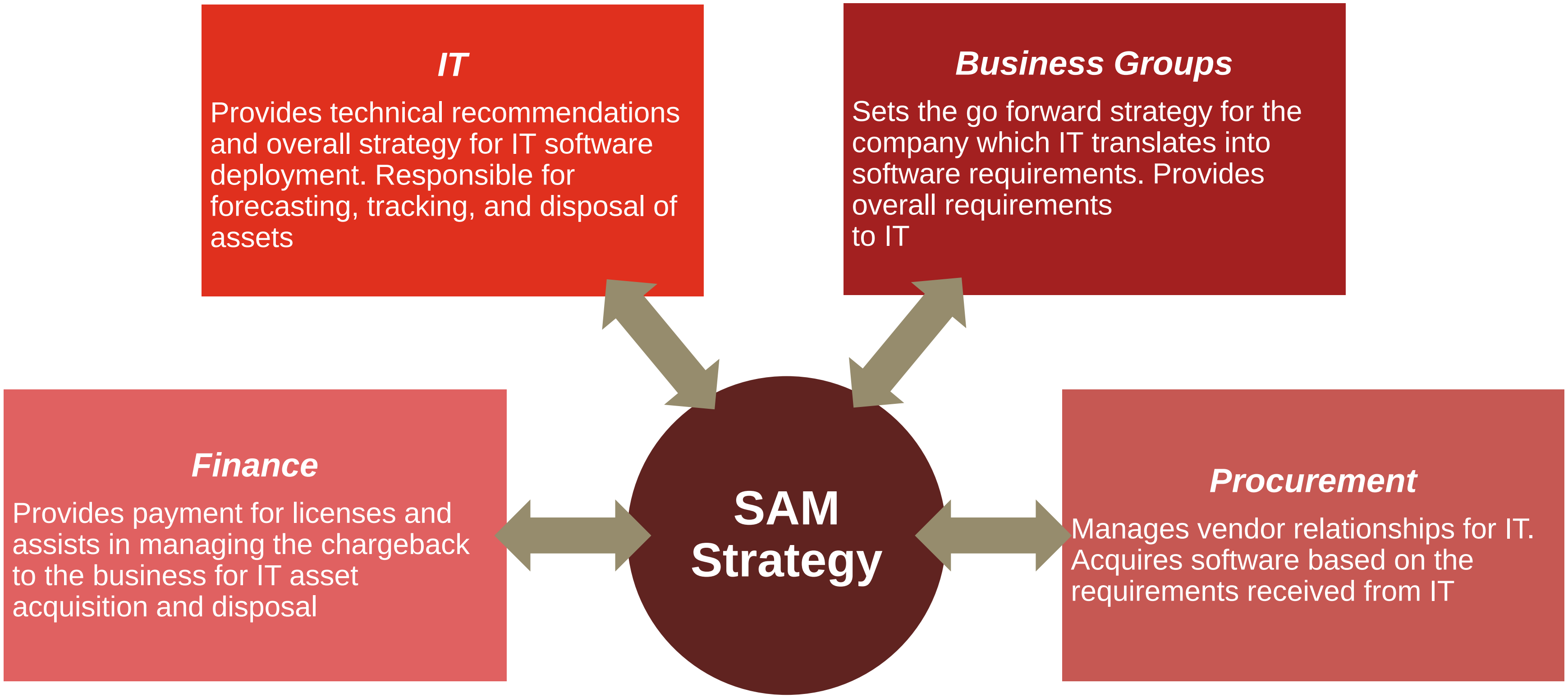
technology

to allow software licenses and usage to be systematically tracked, evaluated, and managed.



Success in SAM

An overall strategy and governance model must be in place for SAM to be effective and to have a common transparent view of services provided. This is dependent on multiple groups working ***in conjunction*** with each other to set standards, policies, and the overall strategy.



IT

Provides technical recommendations and overall strategy for IT software deployment. Responsible for forecasting, tracking, and disposal of assets

Business Groups

Sets the go forward strategy for the company which IT translates into software requirements. Provides overall requirements to IT

Finance

Provides payment for licenses and assists in managing the chargeback to the business for IT asset acquisition and disposal

SAM Strategy

Procurement

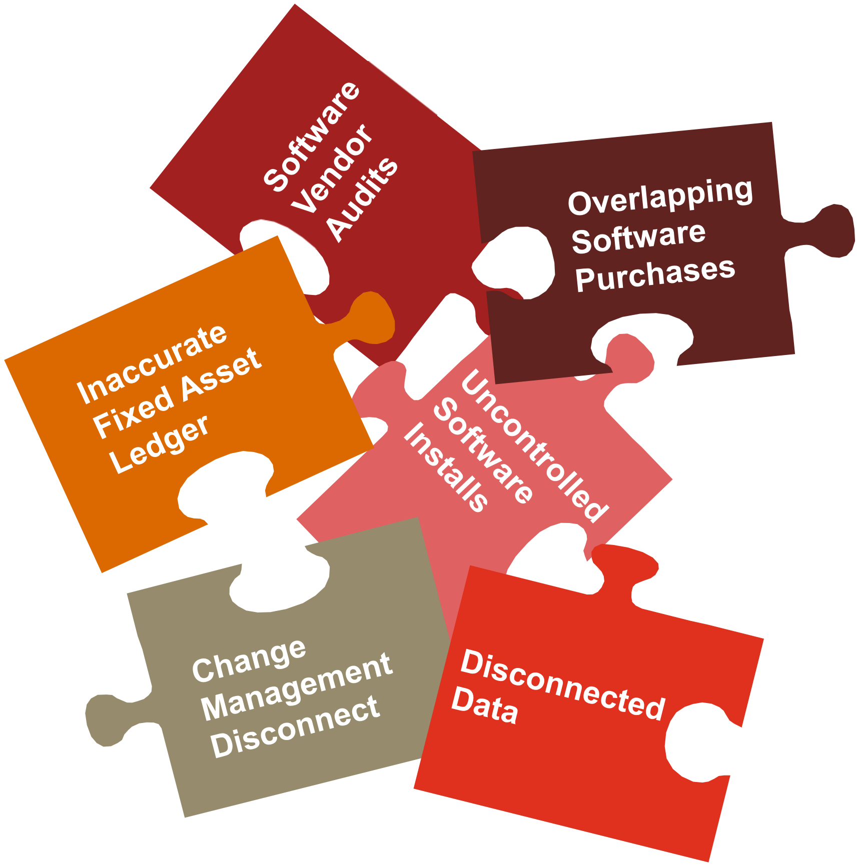
Manages vendor relationships for IT. Acquires software based on the requirements received from IT

The SAM puzzle

One of the major factors contributing to the complexity and increasing SAM Risk are the number of disconnected, disparate, point solution databases across the organization.

Can these questions be answered “yes”?

- Are proofs of software entitlement consolidated and managed across all parts of the company?
- Are there documented controls, policies and processes governing the 3rd party software lifecycle?
- Are sources of truth reconciled (e.g. CMDB, User Lists, HR, Fixed Assets)
- Are there controls to ascertain what is installed in the environment?
- Is there an approved, coordinated software vendor audit response plan?


Software Vendor Audits
Overlapping Software Purchases
Inaccurate Fixed Asset Ledger
Uncontrolled Software Installs
Change Management Disconnect
Disconnected Data

The risk environment has changed

Software audits are an area for Concern

- Your company will likely be audited by one or more software vendors at some point in the near future.

Beware the SAM paradox

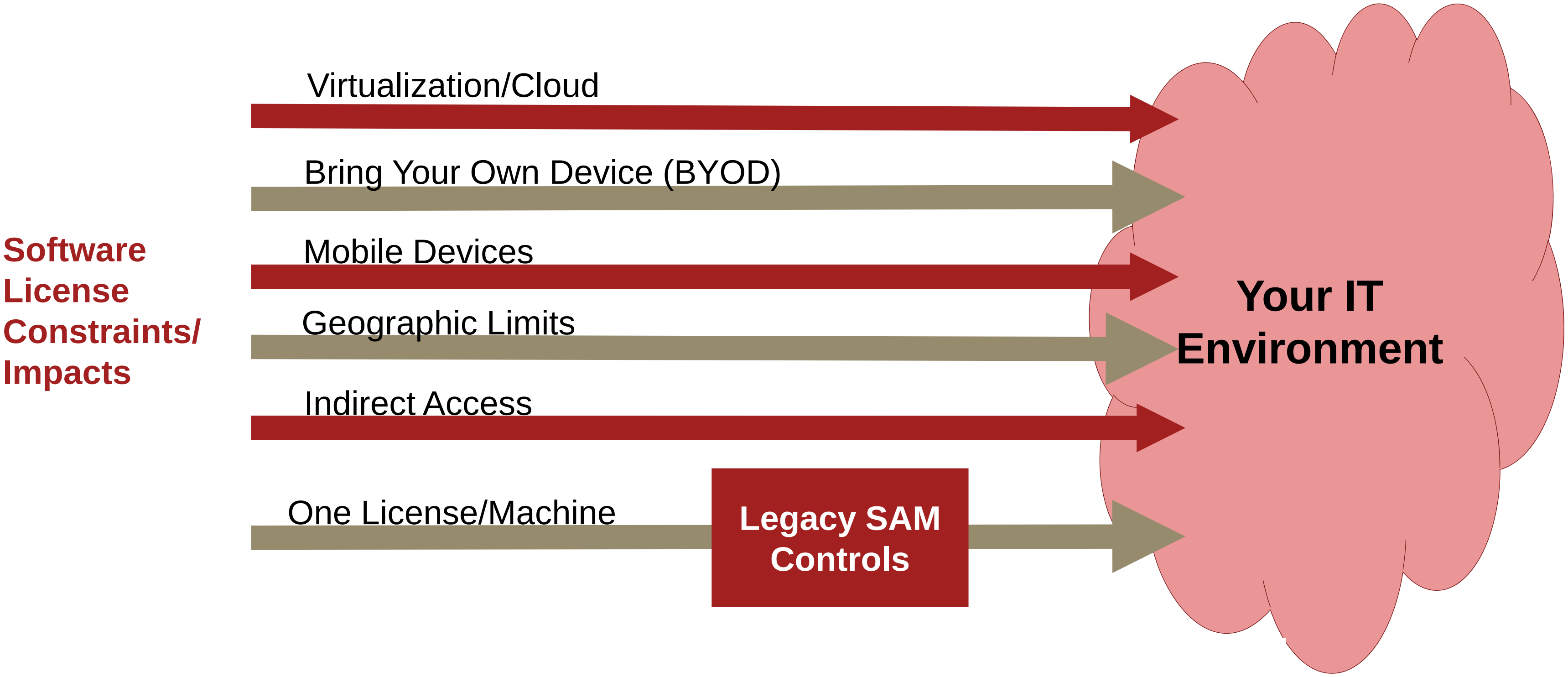
- An organization feels that its licensing data is inaccurate but that it would still pass a software vendor audit.

One software audit may bring others

- Vendor sales teams talk to each other and a big compliance finding by one vendor may bring other audit letters.

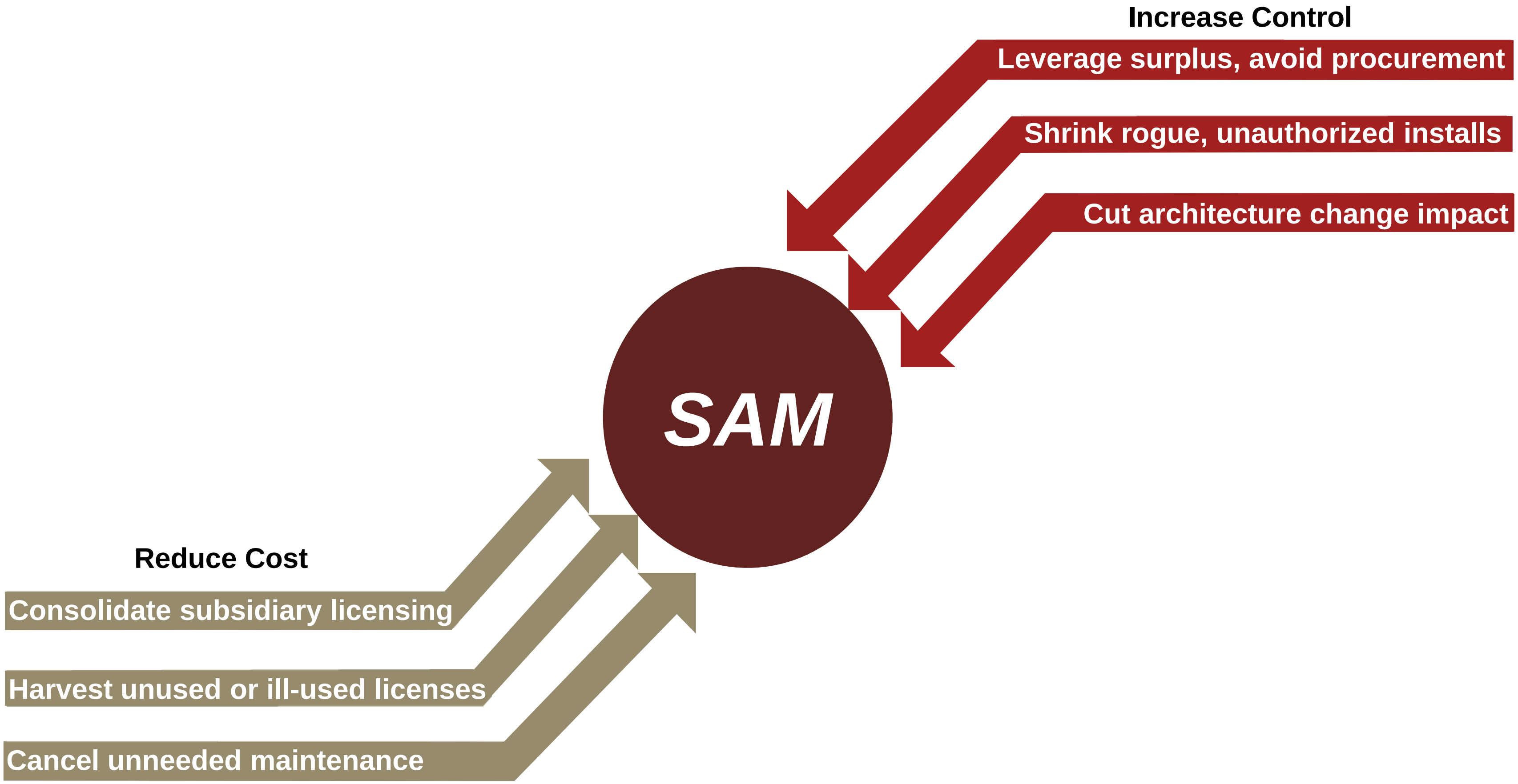
SAM processes may not keep up

The complexity of software contracts and the variety of software license metrics has increased tremendously in recent years. Have your SAM processes kept up? Has your risk exposure increased? Your existing processes may work well for one machine/on license based metrics but not for metrics or environment that included the cloud or geographic limits



The SAM audit opportunity

While there may be significant SAM risks within an organization, there is also the potential for great improvements and increases to the bottom line.


Increase Control
Leverage surplus, avoid procurement
Shrink rogue, unauthorized installs
Cut architecture change impact
SAM
Reduce Cost
Consolidate subsidiary licensing
Harvest unused or ill-used licenses
Cancel unneeded maintenance

Approach

Scope considerations

A key factor in a successful SAM evaluation is determining the scope, including parts of the organization, software and vendors, and which hardware environments/types are included.

General

- Organizational size
- Outsourcing approach

Software

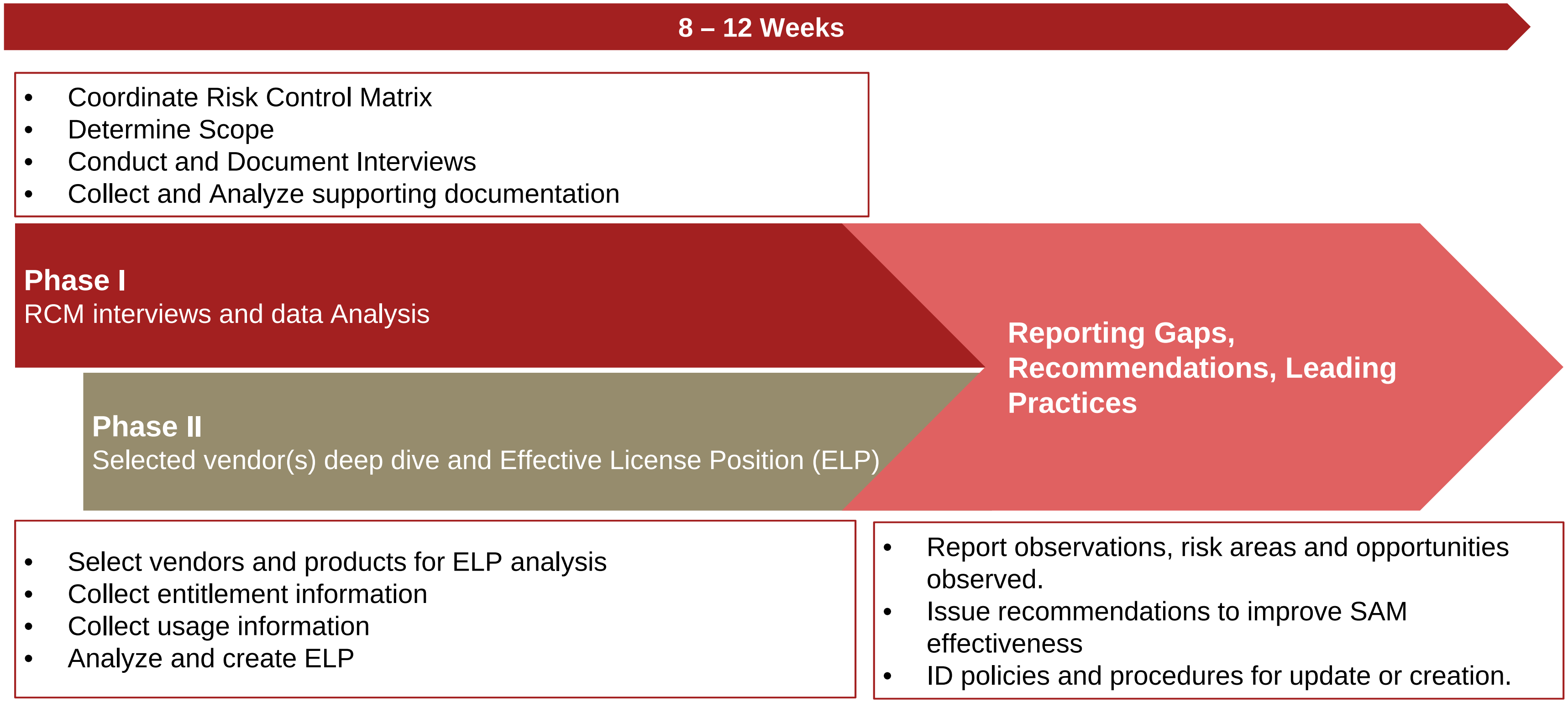
- Amount of decentralized IT management, and ability of users to self-install software
- Centralization, quality, and effectiveness of software entitlement/contract maintenance
- Organizational SAM maturity

Hardware

- Amount of Bring Your Own Device (BYOD)
- Specific hardware classes tracked
- Amount of decentralized hardware procurement
- Coordination between procurement, IT, IT Finance

Combination approach

The combination of a traditional Risk Controls Matrix (RCM) review along with creating a detailed Effective License Position (ELP) for key software vendors/products can provide a more comprehensive and accurate view of the corporate SAM controls, policies, procedures, and implementation effectiveness.



8 – 12 Weeks

- Coordinate Risk Control Matrix
- Determine Scope
- Conduct and Document Interviews
- Collect and Analyze supporting documentation

Phase I
RCM interviews and data Analysis

Phase II
Selected vendor(s) deep dive and Effective License Position (ELP)

Reporting Gaps, Recommendations, Leading Practices

- Select vendors and products for ELP analysis
- Collect entitlement information
- Collect usage information
- Analyze and create ELP

- Report observations, risk areas and opportunities observed.
- Issue recommendations to improve SAM effectiveness
- ID policies and procedures for update or creation.

SAM standards and industry recommended practice

Existing SAM related standards and industry leading practices can provide a good reference point against which to audit your organization but, they must be thoughtfully and selectively applied in order to achieve a greater benefit for the organization.

Standards

- **ISO/IEC 19770-1** - A framework of Software Asset Management (SAM) processes to enable an organization to prove that it is performing software asset management to a standard sufficient to satisfy corporate governance requirements and ensure effective support for IT service management overall. Originally released in 2006.
- **ITIL 2011** - A set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. ITIL describes processes, procedures, tasks, and checklists which are not organization-specific.

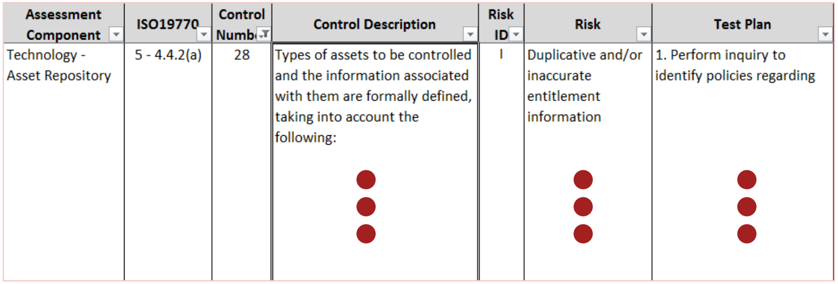
Industry Groups

- **International Business Software Managers Association (IBSMA)** – A nonprofit association of business-focused software asset management (SAM), licensing and compliance professionals. IBSMA works to develop and promote SAM best practices and education.
- **International Association of Information Technology Asset Managers (IAITAM)** - A professional, centralized organization devoted to expanding and codifying information and knowledge within the IT Hardware & Software Asset Management fields

Risk Control Matrix (RCM) component

Description

- Risk/Interview/Artifact Based
- Risk Control Matrix (RCM) developed based on ISO 19770-1
- Controls/Process focused
- Interview questions tailored to roles. E.g.
  - Infrastructure Manager
  - IT Security Manager
  - Software Procurement Manager
  - Desktop Provisioning Manager
  - Legal
  - HR Manager
  - Finance
- Documentation/Evidence request tailored by role
- Output is a final report that highlights areas of SAM risk



Assessment Component	ISO19770	Control Numb	Control Description	Risk ID	Risk	Test Plan
Technology - Asset Repository	5 - 4.4.2(a)	28	Types of assets to be controlled and the information associated with them are formally defined, taking into account the following: ● ● ●	I	Duplicative and/or inaccurate entitlement information ● ● ●	1. Perform inquiry to identify policies regarding ● ● ●

Benefits

- Broader view of processes and controls
- Less impact to customer, interviews only
- More traditional IA risk based approach

Internal audit offerings – Effective License Position (ELP) based

Approach

- Select key software vendors/products based on discussion.
- Pull current contracts and ordering documents from contract repository and determine entitlement based on contract language.
- Leverage existing scanning tools and other third party tools to "discover" product installations.
- Measure product usage for each installation.
- Develop ELP based on entitlements and usage.

Product	Metric	Limited (Y/N)	Deployed	Owned	Difference
Oracle Database					
Oracle Database Enterprise Edition	NUP	N	3,050	1,050	(2,000)
Oracle Database Enterprise Edition (limited)	NUP	Y	0	570	570
Oracle Database Standard Edition	Processor	N	0	4	4
Oracle Database Standard Edition	Processor	Y	0	2	2
Database Packs & Options					
Diagnostics Pack	NUP	N	3,050	850	(2,200)
Diagnostics Pack	NUP	Y	0	190	190
Tuning Pack	NUP	N	3,050	150	(2,900)
Tuning Pack	NUP	Y	0	190	190
Partitioning	NUP	N	2,600	950	(1,650)
Partitioning	NUP	Y	0	510	510
Real Application Clusters	NUP	N	400	700	300
Real Application Clusters	NUP	Y	0	200	200
Change Management Pack	NUP	N	0	150	150
Advanced Security	NUP	N	2.950	0	(2,950)
OLAP	NUP	N	1,300	0	(1,300)
Active Data Guard	NUP	N	900	0	(900)
Middleware					
Internet Application Server Enterprise Edition	NUP	N	360	20	(340)
Internet Application Server Enterprise Edition	Processor	N	0	4	4
WebLogic Suite	NUP	N	1.240	40	(1,200)
WebLogic Suite	Processor	N	0	4	4
WebLogic Suite	NUP	Y	0	150	150
WebLogic Suite	Processor	Y	0	4	4

Benefits

- Actionable reconciliation report
- Real world examples collected for organizations ability to determine entitlement and usage.
- IT gains immediate value
- Quickly shows if existing processes are working

Examples of Results

Examples of audit findings and potential benefits

Every organization is different , however there are some common audit findings and potential benefits.

Sample Findings/Risks

- No defined SAM lifecycle (request to retirement)
- No clear roles and responsibilities
- No maintained source of entitlements
- No “Acceptable Use” policy
- Minimal control or tracking of desktop installations
- Minimal coordination for hardware architecture changes and impact to licensing
- Lack of a software vendor audit response plan
- Lack of trained and supported SAM resources
- Inaccurate financial tracking of capitalized IT purchases
- No software harvesting

Potential Benefits

- Sustainable/managed cost reductions
- More responsive to corporate change
- Enhanced IT procurement visibility
- Better pricing
- Improve license structure
- Volume purchasing
- Reduce redundant applications
- Stop purchasing licenses you don’t need
- Uninstall unused software
- Mitigate compromised data

Role and Responsibility Gap Example

A review of software licensing language (especially renewals) can fall through the gaps between IT, Procurement, Contracts, and Legal.

Geographic limitations

- Usage limited to specified countries or regions
- Usage limited to a certain distance from the installation server

Defined Terms

- “Number of Employees” defined to include contractors, part time workers, or anyone with access to the system
- “Allowable copies” do not include Disaster Recovery sites
- Definitions of User Types

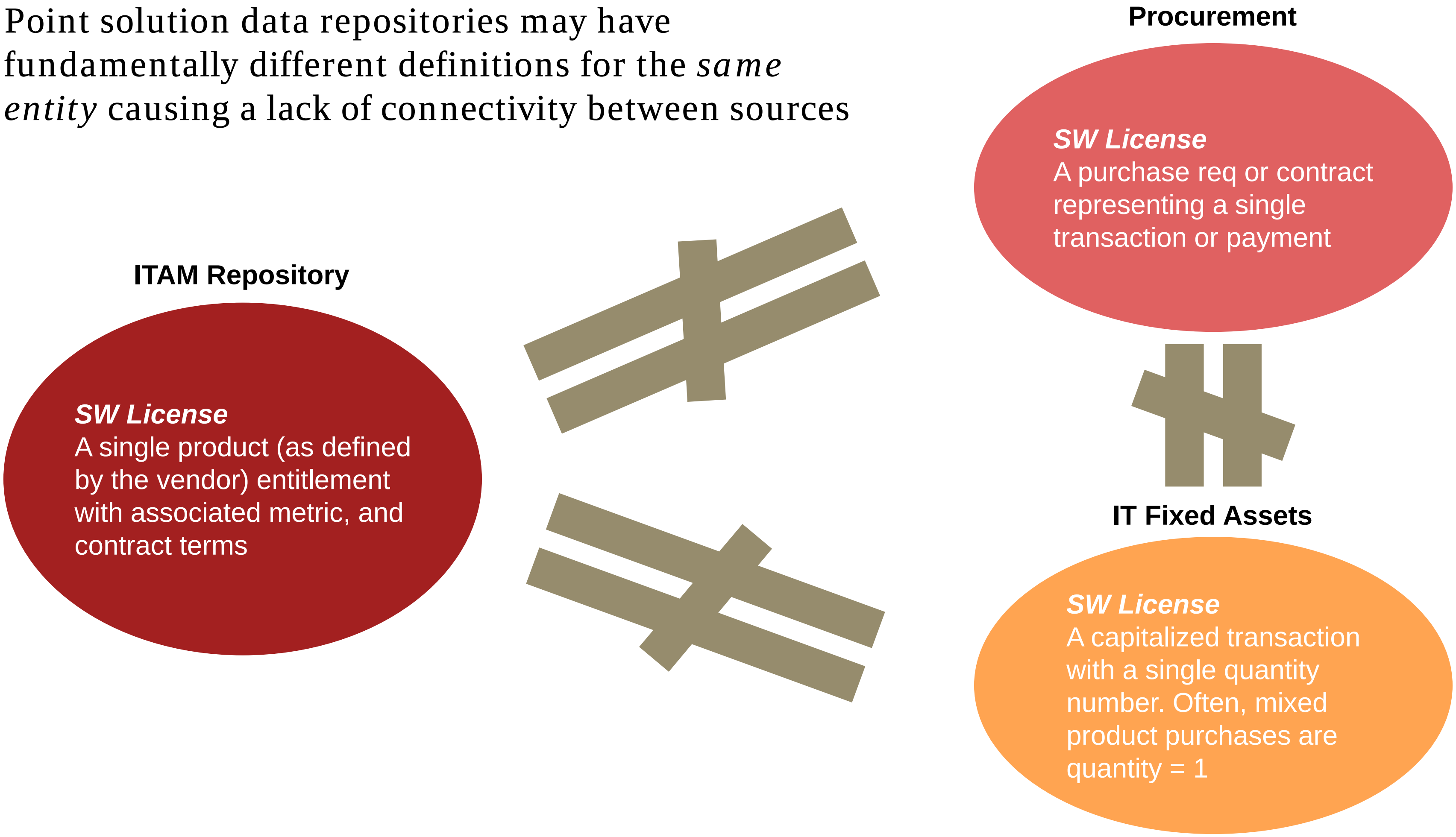
Technical contract clauses that require specialized technical knowledge

- Limitations on accessing data stored in the application (e.g. indirect access)
- Incorporates contents of a continually updated website regarding technical support
- Audit Clauses

Disconnect example – License

Or "What's an application?"

Point solution data repositories may have fundamentally different definitions for the *same entity* causing a lack of connectivity between sources



Procurement

SW License
A purchase req or contract representing a single transaction or payment

ITAM Repository

SW License
A single product (as defined by the vendor) entitlement with associated metric, and contract terms

IT Fixed Assets

SW License
A capitalized transaction with a single quantity number. Often, mixed product purchases are quantity = 1

Inconsistent view of data

Potential Reasons

- Different sources are built for different purposes
- Inconsistent data
  - Different entity definitions
  - Different organizational coverage
  - Different levels of data quality
  - Different unique identifiers
- Scope mismatch
  - Employee Type (full vs contractor)
  - Work from home employees
  - In-stock/stockpiled hardware
  - Restricted use licenses
  - Geography
  - DMZ zones

Potential Disparate Repositories

- Configuration Management Database (CMDB)
- Data Center Equipment List
- Service Desk
- Software Discovery Data
- Procurement Data
- Billing
- Contracts
- Active Directory
- Human Resources
- Facilities

Potential savings from audit results

Four key cost key areas may provide the bulk of the hard $ savings opportunities.

Software Management and Utilization	• Reclamation & reuse of software licenses • Eliminate software overbuy • Promote software compliance
Centralized Strategic Sourcing	• Negotiate, execute, and manage enterprise wide contracts • Lower product acquisition costs • Improved vendor management
Centralized Contract Management	• Lower software maintenance costs • Identification & elimination of redundant products • Improved invoice verification
Software Standardization	• Reduced service calls • Reduced support costs • Reduced operational risk and increased security

Summary & Questions

Summary and conclusion

SAM risks are real

- Software vendor audits are probable and can be a major source of revenue for the vendor. A recent news story related a law suit for hundreds of millions of dollars by a software vendor against a single customer.
- Overspend as a result of uninformed procurement decision
- Inadequate internal controls may allow unauthorized and potentially damaging applications software into the environment.

SAM opportunities are real

- Harvesting software from retired machines or removing when not used can easily save hundreds of thousands of dollars at a large organization.
- Canceling maintenance for unused/retired applications software translates to an improved bottom line.

A combination approach is very effective

- Combining RCM and ELP based approaches yield better results that either approach by itself.
- The ELP can provide hard, actionable data for immediate use.

Questions?