Verifying Asset Accuracy

Q) What is the industry standard way of calculating ITAM accuracy?

Although it might not be the 'industry standard' way, here are some techniques previously used by Martin Thompson (Note: The focus of this guide is to verify hardware).

Verified inventory is one of the seven key ingredients for SAM success:

1. Authority
2. Internal resource
3. Good, verified inventory
4. Good, verified license records
5. A License reconciliation process
6. License expertise
7. Executive group to drive change

Without verifying inventory, IT teams may be sceptical of its accuracy. The International Standard for SAM ISO/IEC 19770-1 is broken into four chunks, the first of which is 'Trustworthy Data'. Without trust, we can't make confident decisions and license reconciliation results won't be strong enough to defend against audits (Software publishers will use their own tools to determine accuracy if your data looks dubious).

Without trustworthy data:

1. IT Asset Managers are not taken seriously. They are supposed to be quartermasters of the IT assets of the organisation, yet they can't demonstrate a good view of assets.
2. Poor data undermines their role and they end up being by-passed on key projects and deployments
3. The ITAM role is seen as bureaucratic – admin with no real purpose – because their data lacks no useful purpose.

So how do we verify asset data to verify accuracy?

There are three primary methods to consider:

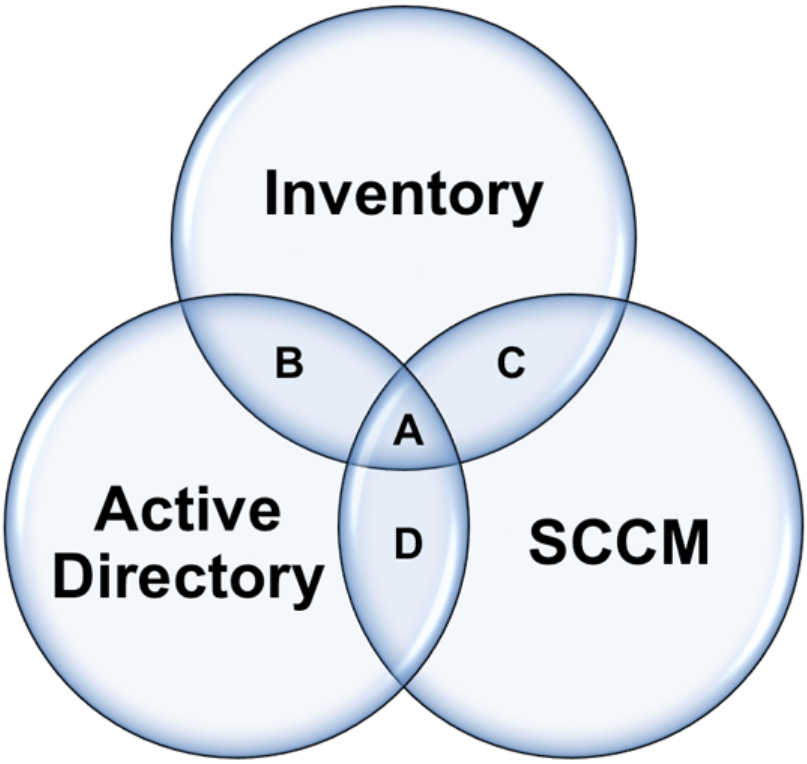
1. Physical spot-checks
2. Lifecycle checks
3. Comparing asset data with other sources

Physical checks
It's always useful to physically 'eyeball' small samples of assets to verify the accuracy of your larger estate. So for example you could go out and verify your records for 20 devices at random and to measure the accuracy of your records.

Lifecycle Checks
Another trick to verify asset accuracy on an on-going basis and constantly cleanse asset data is to ask the Service Desk or other IT teams to verify asset data during their usual day-to-day ITSM processes. For example a service desk analyst could easily verify the ownership of the asset when raising a ticket against it, check department, check the specification or configuration, the data supporting an asset being placed in stock could be checked and so on.

Comparing Data Sets

To verify asset data on a large scale – compare it against other data sets. For example in the diagram below we are comparing inventory data with SCCM data and Active Directory accounts.



This generates some useful disparities:

- **A** – Hopefully this is the majority of your assets. They exist in your inventory tool, Active Directory and SCCM. If you have inventoried assets in this data set who have been seen recently (say within 90 days) and the data has occasional spot checks – I would call this VERIFIED data.

- **B** – The asset exists in Active Directory and your inventory tool, but does not exist within SCCM. There might be perfectly good reason for this – if not this is an exception your SCCM team will want to know about and adds credibility to both your data and your job role.

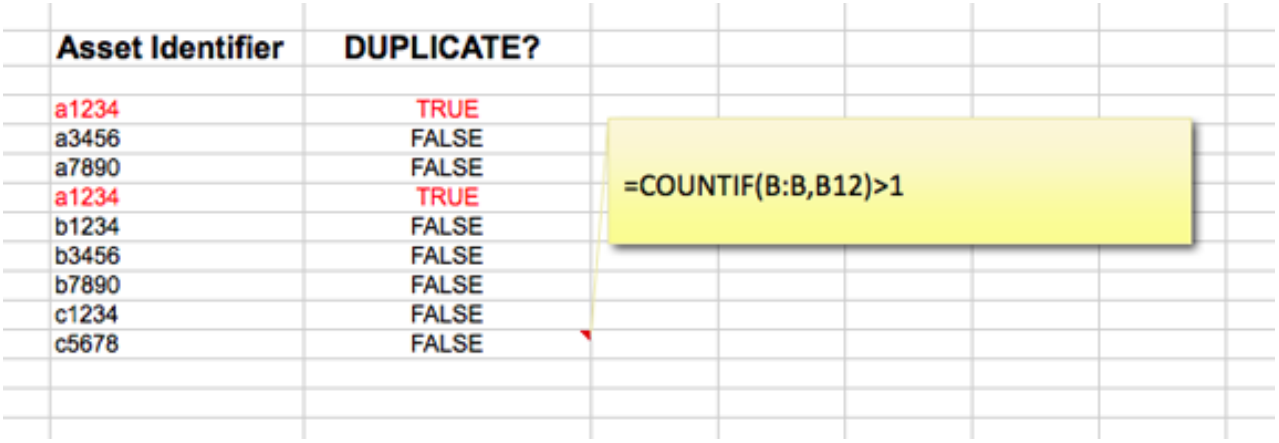
- **C** – An asset exists within your inventory tool and also has an SCCM agent – but does not exist within AD. Again, there might be perfectly legitimate reason for this, if not, this is valuable data for your security team to be aware of.

- **D** – Finally, perhaps devices exist within AD and also have an SCCM agent installed but do not have your inventory tool installed – this is exactly the exceptions you are looking for and addressing them will increase your accuracy.

  You could also use anti-virus, data centre network scans, and comparing SCCM with MAP or any number of others sources to verify data.

  If there is a legitimate reason for a device not being in one of these data sets, it should be recorded in your asset register so you don't need to count it the next time.

Some ITAM tools can help with this verification reporting, but many can't. Whilst a little cumbersome for big networks Microsoft Excel can be used to run the reports. For example =COUNTIF can be used to identify duplicates in a list of assets (Good for cleaning up and verifying inventory) and =VLOOKUP can be used to compare two sets of data and identify an asset that DOES NOT exist in two sets of data.



Continual Service Improvement – Reporting by Exception

The real progress is made with this verification process when it is done on a regular basis. See the report card from a live environment over a 9-month period below. You can see from the table that the organisation is tracking four key metrics in order to verify the quality of asset data.

1. How many devices have we got in inventory
2. How many devices exist in AD but not in our inventory
3. How many devices have we NOT audited (Agent failed, picked up by auto-discovery or network scan but not inventoried and so on)
4. AWOL – devices whereby the inventory agent has not shown a communication or heartbeat back to the server in over 90 days.

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP
Total inventoried devices	22,005	21,074	20,468	20,976	20,626	20,353	19,842	19,240	18,669
In Active Directory but not in Inventory	1,544	2,863	3,115	2,688	2,758	2,758	2,779	2,804	2,867
Unaudited devices	756	599	599	599	595	588	574	557	81
AWOL (not seen in 90 days)	3,532	2,863	2,279	2,279	2,023	1,554	1,187	882	637

Total potential devices	27,836	27,398	26,460	26,541	26,002	25,253	24,381	23,482	22,253
Accurate inventory	22,005	21,074	20,468	20,976	20,626	20,353	19,842	19,240	18,669
Accuracy	79.05%	76.92%	77.35%	79.03%	79.32%	80.60%	81.38%	81.93%	83.89%

Depending on your environment, some may make progress quicker than this, for some it may take a longer. But the most important thing is that we can demonstrate IMPROVEMENT. This greatly increases the credibility of our data and therefore the credibility and usefulness of our ITAM practice.