Do we really need ITAM? Yes!

Johan West, ITAM Forum Ambassador – Fundamentals, and CEO of The ITAM-Unit

In any organisation, we can name things that have value. The people who work for and with us, the money we make, the information we have, etc. Now, imagine if there was no HR department… no central system that holds details on our workforce, who does what, where and when, who gets promoted, who needs what training, and so on. I predict chaos. Now imagine if there was no finance department. Again, I predict chaos.

Now, imagine if there was no ITAM. Tens of millions worth of laptops, servers, stuff in the cloud, with no idea as to where these items are, if they're being used, what they cost, if they've been paid for properly, and what information they hold. Chaos.

We can't afford not to do ITAM just like we absolutely must do HR and finance.

Also, IT assets need to be treated with respect, especially at the point of replacement. Not only because of the information that might be on them but also because of the environment. At the end of their lifecycle, physical IT assets are a form of corporate waste.

Now, caring about the planet might not be a strict and clearly defined legal obligation for organisations in all geos, but I bet most organisations are required by law – or should I say a bunch of laws – to do ITAM for security reasons.

Say what?

Organisations have a number of legal obligations when it comes to IT security and data privacy. Cybersecurity is all about making sure people and systems do what they are supposed to do and especially for systems, that they can't be manipulated, compromised, sabotaged and/or get kidnapped. Aside from very smart cybersecurity professionals, a whole arsenal of software and tools are available to help, such as anti-virus agents, scanning tools, firewalls, intrusion prevention, encryption, SIEM, MDR, etc. Install them in your network, and you're fine. Right?

> "We can't afford not to do ITAM just like we absolutely must do HR and finance."

Well… that all begins with knowing where to install them or what to monitor.

Very smart cybersecurity people agree

Knowing the risks associated with the use of IT and having a very good idea of how 'bad people' go to work to hack, infiltrate, hijack or disrupt businesses, some very smart cybersecurity people have come up with ways to keep us digitally safe. Generally, this comes down to having the right policies and procedures in place and enforcing a number of controlling measures (i.e. Only people we know may access our systems, and then only those people who based on their job are allowed to do so, etc.).

Now, how are we supposed to do that if we don't know what systems we have? And how can we install all these cybersecurity tools on all our systems if we don't know all our systems. In short, cybersecurity couldn't possibly live and breathe without ITAM.

Am I making this up? No. Back to those smart cybersecurity people I mentioned. They came up with a number of methodologies – standards – that are generally deemed 'good'. The ISO 27000 family. The NIST cybersecurity framework. The 18 critical security controls as defined by the Center for Internet Security (CIS18, née SANS20). They all state (in their own words) that everything starts with having all IT assets accounted for – detail everything, everywhere, in real-time what is needed. The CIS18 actually puts this explicitly on top of the list and in others, this principle features prominently, if not conditionally.

But you said law. Yes, for banks in the EU, complying with the ISO 27000 standard is mandatory. US government entities are bound by law to have the NIST cybersecurity framework in place and so are all companies that want to do business with Uncle Sam. In the Netherlands, government organisations must have the ISO 27000 standard implemented.

So yes, ITAM is a definitive must – because cybersecurity is a definitive must.

Did we sign up for this?

If your organisation keeps rejecting your budget request for ITAM people and tools, remind them that they are already signed up for ITAM. Are you using Microsoft software in some sort of volume licensing contract? Do you have beautiful Citrix apps running? Is IBM running in the data center?

It would be fun to show the Boardroom the license contracts typically associated with these software publishers and their products. Any of these – and most others – that license software in a trust model (use whatever you want, just report back to me every year, or variants) have very clear terms and conditions – that your organisation has signed up for. Signed for means agreed to. Signed means legal. So, is ITAM optional?

A lot of fun

Now that you have a couple of sticks at your disposal to get ITAM started or to get budget for further ITAM improvements, let's not ignore the carrots – money. There is hard currency on the table.

Will ITAM lower IT spend? Unlikely. But, ITAM will make sure we spend the right amount of money on IT and prevent wasting precious resources.

> "Cybersecurity couldn't possibly live and breathe without ITAM."

> "Will ITAM lower IT spend? Unlikely. But, ITAM will make sure we spend the right amount of money on IT and prevent wasting precious resources."

The typical organisation without a mature ITAM program

- wastes about $200 USD per year per employee on unused software. (We buy it, we install it, but we don't use it.)
- spends up to 30% more on IT than organisations that have a mature ITAM program in place.

In the first year of operating a mature ITAM program, organisations tend to discover that up to 10% of software maintenance and service contracts are either underutilised or not used at all. Software license audits (not fun) typically consume up to 1,000 internal hours of labour and provide no value to the organisation. It's not uncommon to get three or more of those per year.

With ITAM at a mature level, those are things of the past. Not getting three audits per year saves up to 3,000 hours of labour annually. That should get you a nice $200,000 to $250,000 USD budget to get some people and tools in, yes?