

Technology Asset Management

Workbook

Reducing Tech-Related Costs & Risks

**Basic, Common Sense, Cost-Effective Methods
For Use by Any Business
Right Away**

Produced by:

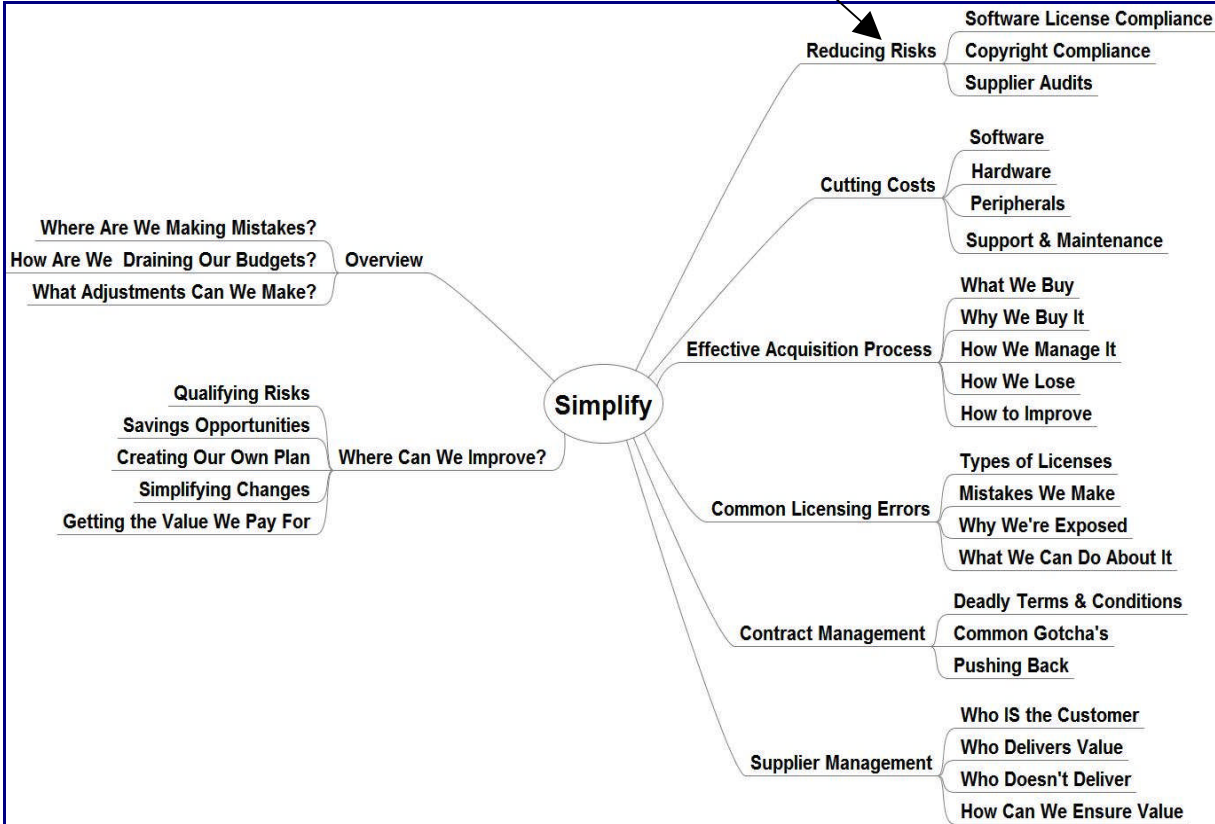
The Institute for Technology Asset Management, Inc.

&

The Business Technology Consumer Network, Inc.

What's this series look like?

You are
HERE!



OK, Plastow! Here's What I Expect:

(Please read over the next few pages before you put your numbers on this one.)

I want to reduce my audit exposure by _____ %.

I want to reduce potential fines/penalties by _____%.

I want to streamline IT spending by _____ %.

I want to improve ROI on my IT spend by _____ %.

And I'm willing to commit to getting the job done!

Tip of The Iceberg

Our time together in this online format will obviously be brief. As a result, we're going to cover only the core issues that you'll need to clarify to get started in reducing technology costs and minimizing risks. Keep in mind that, if we do not cover a specific topic you want to discuss you are welcome to send us an email. We'll do our best to get you the answers you need.

Session One Includes Basic:

Compliance & Enforcement Infrastructure

Follow-Up Sessions May Include:

Software Asset Management

Document Management Process

Support & Maintenance Management

Hardware Management

Contrary to popular belief, you do not have to spend money to establish the core methodologies for saving money across the life cycle of technology portfolio goods and services. A little applied common sense can go a very long way toward establishing the infrastructure to begin minimizing risks while obtaining the value you expect – the value you are not currently obtaining.

However, there is one caveat: (*You knew there had to be a catch or two, right?*)

Realistically, as your technology portfolio management program grows in scope and sophistication, you WILL have to automate the core asset management procedures to ensure maximum accuracy. This means you will eventually want to obtain, and learn to effectively use, automated technology asset management tools. No matter what your relative size, or location, you'll eventually want to acquire and fully implement the following:

- An effective automated configuration discovery tool,
You'll absolutely have to know precisely what's on your systems.
- An effective uninstall tool,
You'll need a dependable way to fully remove products.
- A data repository – anywhere from a basic spreadsheet to full database,
You have to be able to track all IT goods & services.
- A document management methodology – filing system...
You absolutely must keep IT asset-related documents secure.

Begin – now (as a foundation for this session) – considering how much you'd like to save as a % of your IT budget...

And be prepared to write it down – because we're discussing how it's done!

Compliance & Enforcement Infrastructure

Since the mid-90's many of the collective industries representing copyright-protected products have apparently determined that customer goodwill is less important than the revenue generated from punitive enforcement initiatives.

Licensing and other agreements have gone from “competitive differentiation” to “rights compliance” nightmares. As business technology consumers, we have permitted onerous license terms and conditions to be the rule rather than the exception. As a result, we have become easy, and very lucrative, non compliance audit targets. This section is a very basic introduction to the major risk issues and risk mitigation methodologies that you can use to begin protecting your enterprise with a “wall of due diligence” between you and the predatory enforcement audit players.

Warning – As many as 50% of American enterprises may be targeted for supplier audits during any given 18 month period. American companies – with one of the lowest piracy (non compliance) rates in the world – are not only the most frequently audited but we suffer the most significant financial penalties. Will you be prepared to deflect the auditors when they contact you?

Issues to Consider:

First – Clarify & Minimize (or Eliminate) The Risks – This is where nearly every company begins the asset management journey. True to human nature, we generally fail to recognize and confront problems until they surface, become our own, and escalate out of our control.

Key to Success? When you proactively establish control over your technology portfolio you will immediately begin saving money (as much as a 25% reduction in technology spending in the first year). If you wait until you are confronted for audit, the reactive processes will cost you significantly more- and you'll still eventually have to put IT asset management in place. It just makes sense to manage IT goods & services BEFORE you are forced to do so.

Risk Products? Virtually any product that is covered under national or international copyright law can become a serious risk to the enterprise. These include operating systems, software, fonts, graphics, audio, video, photographic images, print documents and images, even games.

Key to Success? If the same products and software industry players show up in the majority of punitive audit announcements, wouldn't it make sense to either avoid these products and companies, or focus more closely on controlling their products?

Potential Price of Ignoring This Step? License non compliance and piracy fines with related penalties that can easily exceed \$2,000 for each computer your company owns. Count your computers and do the math... Damages also include loss of negotiation position for future IT purchases and potentially serious damage to the enterprise name you worked so hard to establish.

Key to Success? The average enforcement audit can easily cost even a small company in excess of \$100,000. Enforced repetitive audits and associated ongoing costs can add nearly double. Establishing your own controls, and doing so proactively, can virtually eliminate these forced losses.

Cost to Correct? Minimal – No new software or hardware to acquire to get started. No new consulting services. At the front end, compliance assurance can be nearly all brain work – employee time – establishing a document management process, populating the information, confirming the products that the enterprise genuinely possesses.

Key to Success? *The most critical element of the compliance enforcement audit involves the processes of collecting and organizing key documentation. Doing this in reactive mode is always significantly more costly than doing it on your own time and at your own pace. Correct the basic problems before being forced to do so by an outside threat. THEN step back and re-enforce your asset management infrastructure into a more powerful “wall of due diligence.”*

Audit Letter Example - Before we get going, read the sample audit letter on the next page. Can you spot the traps and pitfalls? Tens of thousands of these are sent out every year. Some audit notification letters are nothing more than phantom “fishing expeditions” - some are frighteningly real. Get comfortable with the language and underlying threats – you'll probably see one of these for real someday in the very near future.

Key To Success? *Remember: in this first session, we're only focusing on plugging the defects in your due diligence so you minimize your punitive audit exposure. What is really great about what we're about to cover is that you will use nearly every element we discuss as part of your IT life cycle management foundation. Doing this proactively will put you on the road to value more quickly.*

Now... Read the letter.

But, don't panic. We'll walk through this with you.

Additional information & strategies are available at <http://www.biztechnet.org>

Sample Enforcement Audit Notification Letter

Mr. or Ms. CEO,

We have evidence that Your Company, is engaged in the unlawful copying and use of our software in violation of the Copyright Act, Title 17 U.S.C. 501, et seq. We settle most instances involving copyright infringement based on the following terms:

- A. Your Company immediately conducts a computerized audit of the software on all of its computers and servers using Audit Software we supply.
- B. Your Company furnishes the software audit results along with copies of the user's software licenses and documentation showing date of purchase.
- C. Your Company agrees to pay a negotiated amount based on the numbers of unlicensed copies software reflected by the audit.
- D. Your Company destroys all unlicensed software and agrees to refrain from further use of unlicensed software in the future; and
- E. Your Company agrees to implement a software license compliance program; and
- F. We will release Your Company from all claims and causes of action for copyright infringement of the software listed on the attachment to this letter.

In the event Your Company is unwilling to settle in accordance with these terms, the judicial remedies available under the Copyright Act include statutory damages up to \$150,000 per violation for willful violations and \$30,000 per violation for non-willful violations, plus attorneys fees and an order requiring the destruction or other disposition of all copies found to have been made or used in violation of the copyright owner's exclusive rights. Title 17 U.S.C. 502-505.

We will not hesitate to enforce our rights through litigation if this case cannot be promptly resolved in accordance with the terms enumerated above. Please call me immediately, or have your company's attorney call, to discuss whether this case can be settled without seeking judicial relief.

In the meantime, Your Company should not delete or remove any unlicensed software from its computers or servers. Evidence of unlawful use of software will be material to any litigation which may ensue, and your negligent or willful destruction of such evidence will give rise to an independent cause of action for spoliation as well as claims for compensatory and punitive damages.

In addition, please do not license or enter into any negotiations to purchase any computer software products prior to the resolution of this matter. Either purchasing licenses or deleting software at this point will not remedy past unauthorized installation or use, will not conclude our investigation and may prejudice our ability to reach a mutually satisfactory resolution.

I will contact you in the near future to discuss how Your Company wishes to proceed. Meanwhile, more information about my software publishing company, and its affiliates, is available at www.____.____ and more information about _____, the _____ authorized audit tool, is available at www.____.____.

Very truly yours,

Software Industry Lawyer, Esq.

Section One Q&A – (*As much as we can pack into the next 50 minutes.*)

You may not need to know these answers today but you will need to be very clear about the facts when the auditors come knocking... THESE items represent the most basic level of your compliance assurance “wall of due diligence.”

You Are Being Hunted -

Who are the people who will audit your company?

Where do they get the power to audit you?

What is the difference between non compliance & piracy?

What are your chances of being targeted for a vendor audit?

What laws, regulations, and governmental Acts impact your acquisition, use, and disposal of technology goods?

What are the potential fines per copyright violation?

How would you calculate the approximate actual costs of a non compliance audit?

How do these enforcement auditors locate your company?

Statistically Speaking:

As many as 1/3 of the average organization's IT assets are not tracked.

Source: Info-Tech

Rewards! (*Whistle-Blowers: Get Rich, Quick*)

Why is “compliance for the sake of compliance” a waste of your money?

How do the licensors blindside the business software consumer?

What are the compliance assurance rules?

Who monitors and/or regulates the auditors?

And what does that mean in terms of your rights?

[Now let's step through some enforcement audit details](#)

What product lines are most frequently cited during enforcement audits?

How could you use this information?

Which ones are actually on your systems?

When were they placed on the systems?

Who put them there?

Where are those systems located?

Who is using them?

Statistically Speaking:

Enterprises with effective SAM establish a 23% edge in revenue per employee.

Source: Keystone Strategy

How can you win the document management shell game?

What documentation will you need (but most likely not be able to find)?

Proofs of purchase...

Proofs of authenticity...

License...

Registration...

Master Media...

Manuals... (Seriously... Manuals?)

Playing Audit Reconciliation Bingo

Got your Bingo card ready?

Interacting with your (former) friends

Communications

Details

Negotiations

Pushing Back (*Carefully...*)

Don't Let Them Kid You: They'll be back... And so will their friends...

Statistically Speaking:

Enterprises with effective SAM enjoy an 8% to 15% reduction in acquisition costs.

Source: Gartner

Notes, Additional Information. and Questions You Would Like Answered

Remember something you wanted to ask? Send us an email & we'll do our best to fill in details. This information in no way guarantees that you will not be targeted for audit. Nor does it imply how well or poorly you will fare with the audit agency or group during an audit. We do not provide legal or auditing advice. Use at your own risk. Always consult with your legal and/or accounting professional prior to utilizing this material.

We provide supplier- and product-neutral asset management methods based on practitioner-proven processes and procedures. Neither The Institute nor The Network is affiliated with any supplier of technology goods or services.

Coming Up in Our Cost and Risk Reduction Series:

Software Asset Management

Document Management Process

Support & Maintenance Management

Hardware Management

Additional Topics Available

Audit-Related Reports You'll Want to Be Able to Generate

(This is NOT a comprehensive list but it'll get you way ahead of the game.)

Also, THIS is why you will eventually want automated audit software.

Copyright-Protected Products Loaded

Sorted by Copyright Holder

Sorted by Specific Product

Where Each Product Is Located

Precisely what computer – location / MAC address

Primary user of product loaded

When installed & by whom

Date & results of last internal audit (maybe even two or three)

Precise Documentation – This is also how you'll set up your filing system.

Proofs of purchase for each specific licensed product

Proofs of authenticity for each product requiring them

Licenses for each product & proof that you are using according to license

Registration details & related documents

Master media and (if required) manuals or manual excerpts

Do NOT forget that there are other copyright protected products besides software and that their copyright holders are also more than willing to conduct punitive audits. Start tracking music, graphics, fonts, video, print media, and other potential target products. No need to panic – Just begin putting the proactive processes in place.