



IT Security Compliance Management can be done right!

(and make sense doing so)

Hi.

My name is Adrian Wiesmann. I work as an IT Security Officer for a Swiss Financial Institute and my daywork is ~~to bother, to pester and to annoy~~ to help make the companies systems secure.

Agenda

- Common Problems
- Solving Strategies
- Suggested Solutions
- The Future

Todays agenda is as follows:


- Common problems to compliance management
- Solving strategies to cope with the common problems of compliance management
- Solutions we follow with SOMAP.org to get things working
- Where we are heading to next

Motivation

Overload
is not an
option



The Problems with Compliance Management



Problem #1

The Amount of Controls

7

There are just too many authority documents containing too many controls. Depending on the size and the industry of a company different authority documents have to be considered. Many of these contain completely different controls. They are usually not harmonised or aligned with each other. Many times different controls from different authority documents are somehow affect each other. And of course, different authority documents seldom reference each other.

Which brings me to these questions:

- Which of these authority documents are relevant (and why)?
- Which of the controls in these authority documents are relevant in your situation?
- Who in your environment is affected by these controls?
- How does this look in the future?



Problem #2

The Disorder

8

Compliance management is like trying to bring order into a haystack. Or a box of ropes. Or both.

Different authority documents with different controls provoke some incertitude.

Now that you know which authority documents and controls are relevant.

- What does this mean for your environment?
- Which assets do you have?
- Who is responsible for these assets?
- Do asset owners know which controls are relevant for them?
- Which authority document version is the latest? Who takes care of keeping up to date?
- You need some internal document management.

Which means that it is the responsibility of the user of authority documents to bring order into this disorder. We will talk about some strategies how to do so.

Problem #3

Compliance isn't cool

or that's what the cool boys say...

Oh how we laughed...



Even a short film exists where it is explained how security vs compliance looks like. It is explained with a motorcyclist once wearing full leather and the other time full... helmet and sunglasses.
Oh how we laughed when watching that film!



Unfortunately all of these miss the point.

Of course you can do compliance management in a way that you only do what you are asked (or forced) to do. As much as you can do business without listening to your customers.

But does this count as due diligence and due care?

Compliance management is not about only following whats written down somewhere. For me compliance management is about knowing

- what your company is about,
- what your environment is about,
- what assets you have,
- why you have them,
- how these play together,
- how much worth they are, etc.

Compliance is about knowing and focusing on your environment.

And this talk is about making sense of compliance management and thinking out of the box.



Problem #4

Many miss the point

but at least they are compliant doing so :)

So we wanted to
change this.

We noticed this some while ago. So we wanted to change this.

we, SOMAP.org



We means, the Security Officers Management and Analysis Project - SOMAP.org

SOMAP.org focuses on the **Security Officers** and on helping them in doing their daily business as comfortable as possible.

The main goals of SOMAP.org are to develop and maintain:

- **Guides and Handbooks** explaining and describing Risk Management.
- an open and free 'best practice' **Risk Model Repository** with security objectives, threats and other risk related meta-data.
- an open source **Security Management Tool** which is making use of the meta-data from the projects own risk repository.
- **Report Templates** which can be used during a risk assessment process.

Main Goals

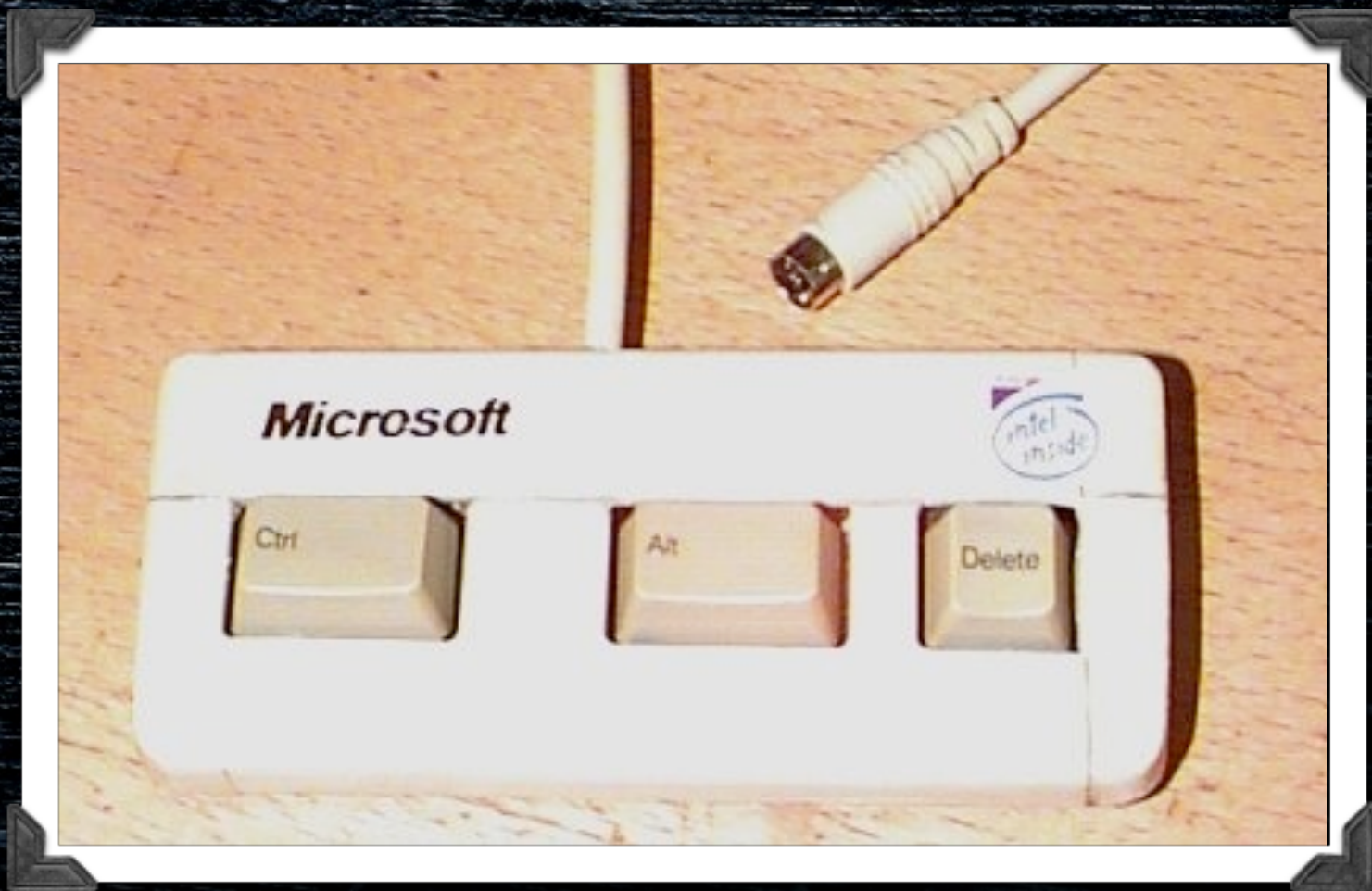


Goal #1

Don't reinvent the wheel

Goal #2

Make things simple



Goal #3

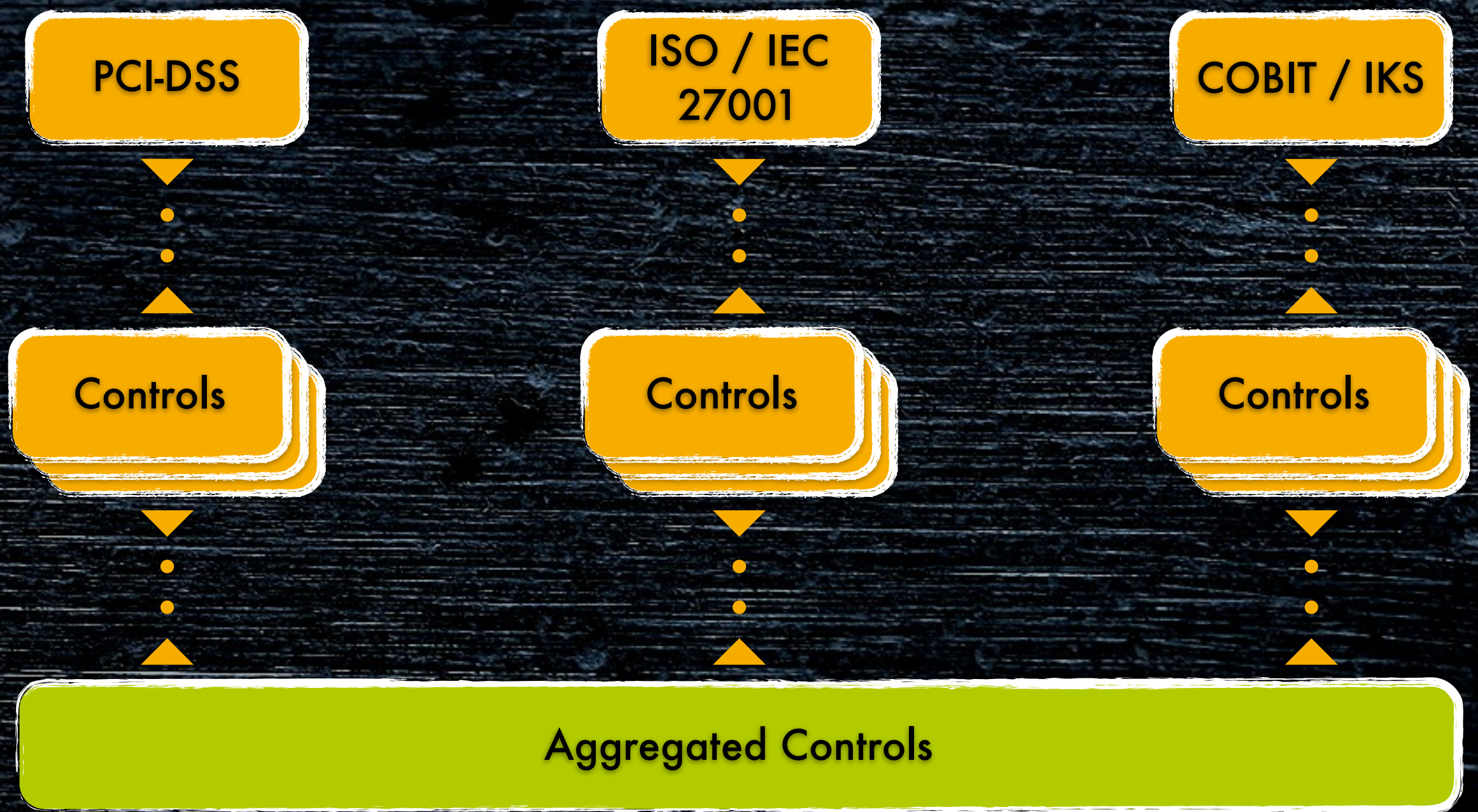
Thinking outside the box



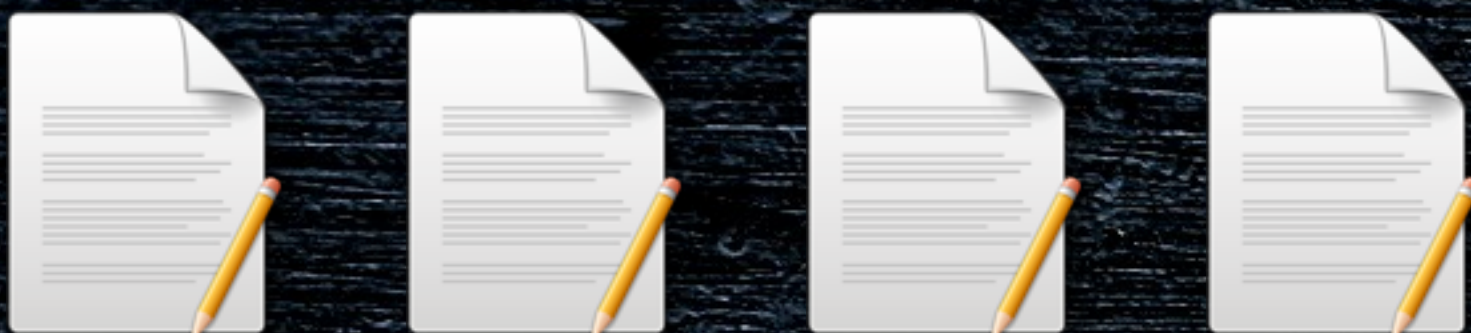
Our Approaches

So here are the approaches we follow with SOMAP.org to make things manageable and simple.

Strategy #1 Aggregation



New Catalogue



Catalogues



Remove
duplicates



Aggregated
catalogue

Master Catalogue



Weighting



Catalogues



Remove
duplicates,
weighting



Aggregated
catalogue

This aggregation type is by far the most complex one. There is no master catalogue but we do work as in aggregation type 1. The main difference is that in this aggregation type we weight all the controls. So if we have multiple controls which are about the same topic, then we weight which control we take.

Worst of all. While this aggregation type makes the most sense in many situations. It unfortunately does not scale well. Think about a common company with (only) 4 relevant authority documents. Working through all those authority documents and all these controls can be very time consuming and generally a royal PITA.

Shopping



Buy Catalogue



Aggregated
catalogue

Luckily there is also the option to shop for aggregated control catalogues. There is a company selling a pre-aggregated catalogue. It is called the Unified Compliance Framework (UCF) and they state that their Framework “[...] is the only [...] compliance database that reduces the regulatory maze to a much smaller set of ‘harmonized’ controls”.

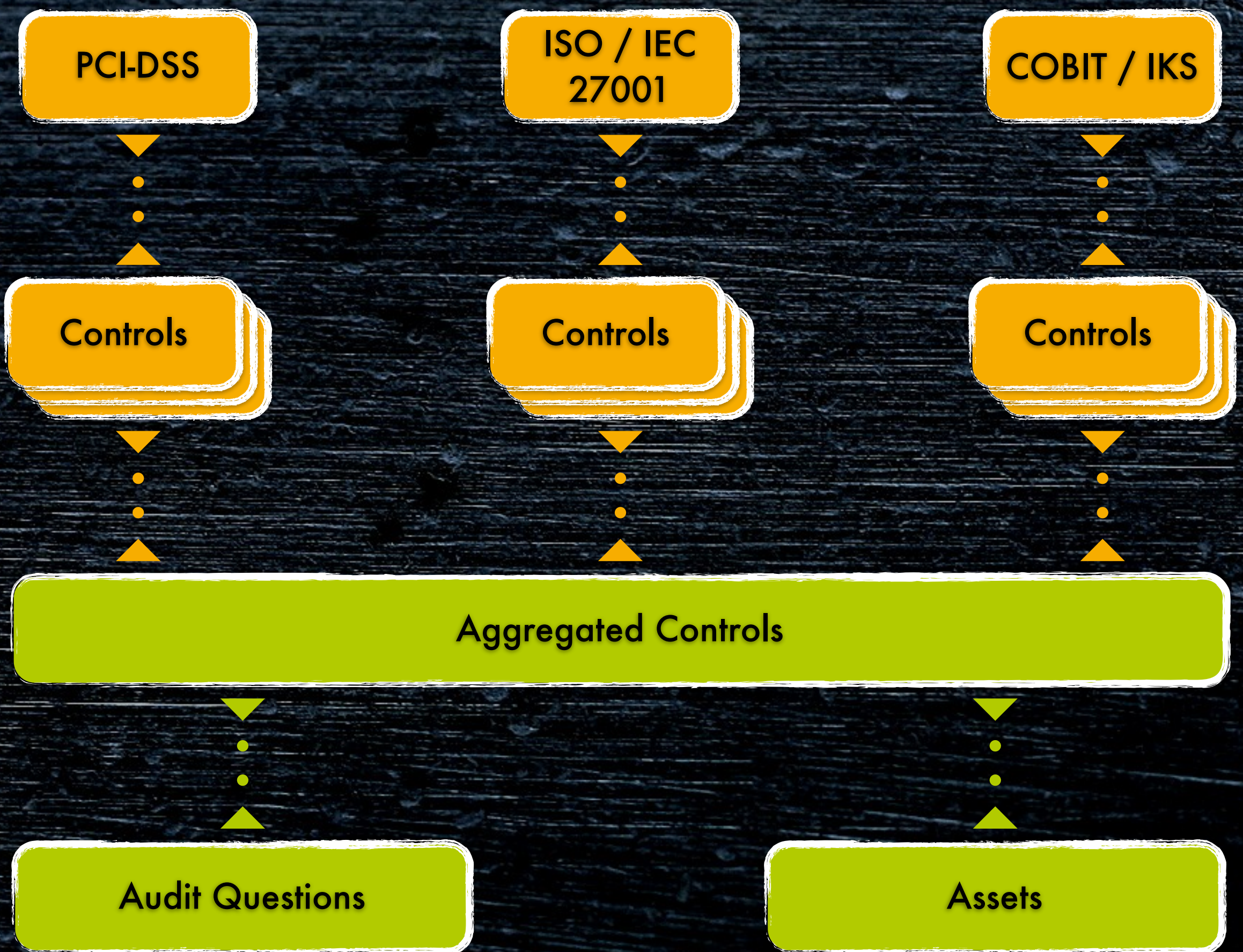
The UCF talks about harmonisation, but after all they just have their own catalogue and make sure that every major authority document is taken care of.

It is very important to note here, that even when you go and buy that UCF, you will always have to work yourself through the whole set of controls. The UCF is not a catalogue of its own but an intelligent mapping information. But at least you have some guidance on:

- which authority document versions are the latest,
- where do you get the authority documents from,
- how do they influence each other,
- what are the intersections.

Strategy #2

Self Assessment



For the self assessment, the aggregated controls are linked with audit questions and assets. With these links we can automatically determine which audit question is relevant for which control for which asset type.

Strategy #3

Meta Data Model

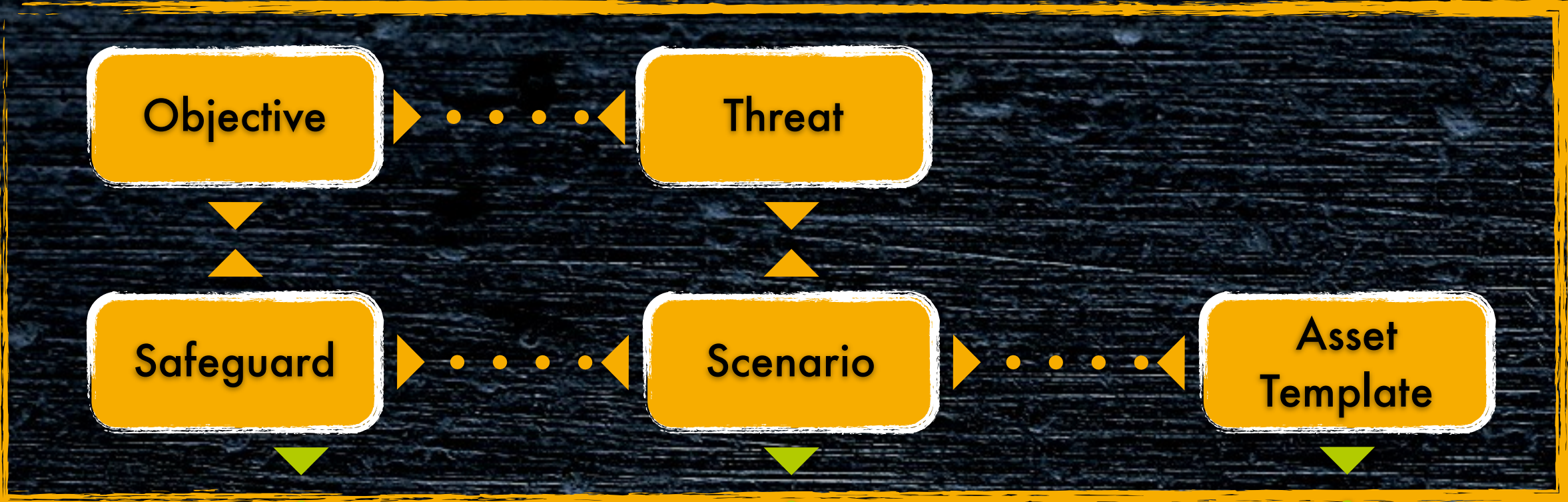
Strategy #4

Reuse the Meta

...for Risk Assessments



Model



Instance





Strategy #5

Don't do silly calculations

Strictly no silliness

- No percentages for degrees of realisation
- No risk calculations based on... best practice
- No magic
- No solitaire



34

Maturity is not measured in percentages. When is a task 50% done? Isn't MS Project or another tool better to track percentages? Has somebody failed PCI-DSS by 43%?

Tracking of safeguards can either be done on every safeguard, or on a company wide level. Let's say some controls are fixed / implemented on a company wide scale. Why should every asset owner track this on her own?

Regarding the risk calculations. Have a look at the Intel Threat Agent Library. This is a catalogue of threats, agents, enablers, skills which taken together are quite similar to CVSS.

Best practice means everybody does it. But does it have to make sense only because of this? Think out of the box!

And regarding the solitaire. We should focus on the tools functionality and not add a solitaire, because we can...

What the future brings



Metrics

The screenshot displays the Metrics Center interface with three main panels:

- Contexts:** A tree view on the left showing various security standards and frameworks, including PCI DSS v1.2, NIST Metric Type, NIST SP800-53 Controls, and ISO/IEC 27002. The '11.2 User access management' item is selected.
- Search Results:** A central panel titled 'Advanced Search' with filters for 'Owned by/Visible to', 'Dates', 'Popularity', and 'Full Text Search'. Below the filters, a list of search results is shown, including 'accounts-per-user', 'password-policy-coverage', 'password-expire-coverage', 'strong-auth-coverage' (highlighted), and 'accounts-closed-correctly'.
- strong-auth-coverage:** A detailed view of the selected metric on the right. It includes fields for Name, Version, Owner, Group Owner, Rating, Views, Created, Updated, Title, Status, Units of Measure, Targets, Description, and Objective.

strong-auth-coverage Details:

- Name:** strong-auth
- Version:** 0.1*
- Owner:** 6AC5:eJyz4t
- Group Owner:** --public--
- Rating:** ★★★★★
- Views:** 41
- Created:** 2009-01-25
- Updated:** 2011-09-19
- Title:** strong-auth-coverage
- Status:** Draft
- Units of Measure:** Percentage of Critical Assets
- Targets:** 100%
- Description:** This metric measures the percentage of systems with critical information assets that use stronger authentication than IDs and passwords in accordance with policy. Note: A user name and password is called "single-factor authentication" or "weak authentication." Strong authentication requires using at least two of a possible three factors: something you know (a user ID, password, or PIN), something you have (a security device you plug into a USB port), and something you are (a retina scan or fingerprint). Therefore, an example of strong authentication would be a password (something you know: factor #1 and a fingerprint (something you are: factor #2).
- Objective:** This baseline metric measures the extent to which authentication that is stronger than one-factor authentication has been implemented for critical assets.

36

Metrics are an important tool to define the maturity. And it is possible to answer audit questions automatically with metrics. Because of that asset owners need to answer less audit questions, making things even simpler. No need for manual answering if you already have the data to answer it for yourself.

There are some (public) projects working on metrics:

<https://www.metricscenter.net>
<http://securitymetrics.org>

Connecting metrics to aggregated controls opens up the possibility to automatically answer audit questions or to check the quality of manually filled out audit questionnaires.

Evidence



37

Evidence is everything an asset owner or custodian can show as proof that they did implement a control or safeguard. Evidence can be manifold: Documents describing a process, some hardening document, config files and other data.

We started to use a JCR repository to the ORICO Tool to be able to store such evidence. Now there is that discussion if it makes sense to integrate such data into an audit tool or if we only should link said data. But nevertheless this discussion turns out. It makes sense that you can proof that this or that evidence was available on a given point in time. Of course you still need your document management process in place which helps you in regularly keeping your documents up to date. But at least you have the chance to link what you have written with the controls which required you to write that document in the first place.

Questions



Thank You!

Adrian Wiesmann
awiesmann@somap.org