

## IT Security Compliance Management can be done right!

(and make sense doing so)

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

Hi.

Adrian is working as an IT Security Officer for a Swiss financial institute. His dayjob is to bother, to pester and to annoy. Every single day he works hard to bring these qualities of his to perfection. With a background in software engineering he focuses on application security and software demolition but enjoys a fine hardware hack or a well executed social engineering stunt as much as everybody else does. He is one of the founders of SOMAP.org, a non-profit organisation which is authoring and publishing documents and tools for analysing and managing IT security risk and compliance with regulations and standards. Adrian holds a masters degree in information security from the Royal Holloway, University of London.

# 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

3

# Motivation

What is my motivation for this talk?

#### Overload is not an option

I want to make things simple. Overloading stuff is not a solution. We already have crowded working days so simplifying things leaves more time to focus on the really important stuff. This talk is about making some things a little bit simpler.

# The Problems with Compliance Management

This first part of my talk is focusing on the problems we have with compliance management. We will talk about what problems we have and why we have them.

# Problem #1 The Amount of Controls

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 are 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...

And yes, compliance management is not cool. Or this is at least what all the cool boys say. Compliance is an "assault on reason", bashing compliance programs is quite common.

# 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!

#### ...but missed the point

8

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 :)

Have a look at todays literature, whitepapers, whatnots. Many of these just state the same since many years. You have to do this, you have to do that. There is no evolution, no thinking out of the box.

# So we wanted to

# ange ins.

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

## we, SOMAP.org



HOME

Home About SOMAP.org Contact

RISK METHODOLOGY (OGRCM3) RISK MODEL (ORIMOR) RISK FRAMEWORK & TOOL (ORICO) LIBRA

Security Officers Management & Analysis Project

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

Let's talk about what to change or how to change things for the better.

### Goal #1

## Don't reinvent the wheel

I don't want to reinvent whats already there. Let's focus on what is not there yet and on integrating all of the existing parts with all the missing parts.

# Goal #2 Make things simple



As I mentioned in the beginning: It is one of my goals to make things simple. I do not want to make everything as simple as possible but I want to change the important parts as far as it makes sense to do.

17

# Goal #3 Thinking outside the box



Let's not blindly do what everybody else does but let's take one step back and think about what should be different, what does not make any sense, what should be changed. And then only change that one, keeping the rest as it is.

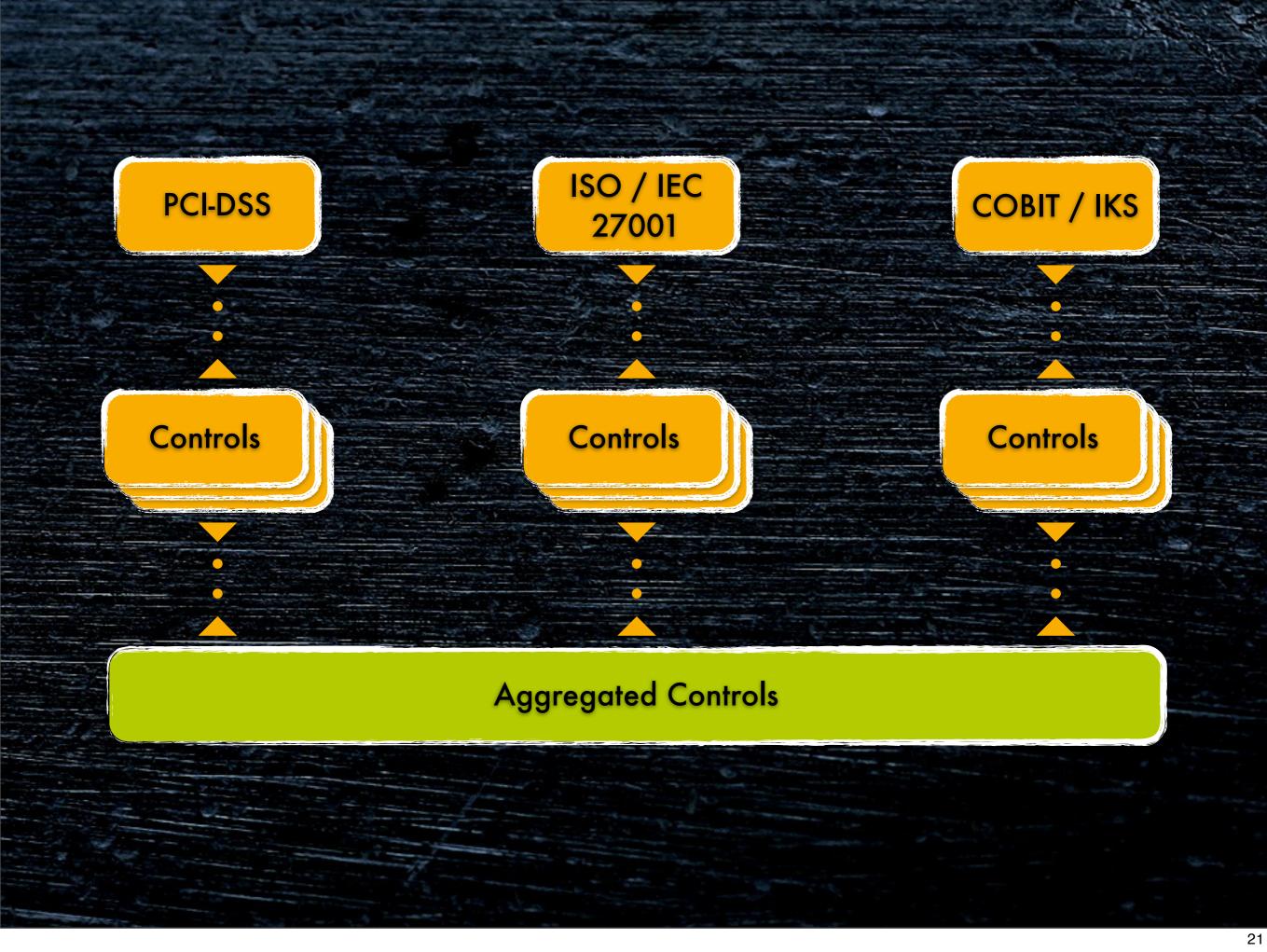
# Our Approaches

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

# Strategy #1 Aggregation

Strategy #1 is all about aggregation. The next slides are explaining what we mean with aggregation and what aggregation strategies there are. And which of these can make sense in what case.

20



Aggregation is all about minimising the amount of controls. It is about removing any doubles and therefore lowering the total number of controls you have to consider. You have to make sure, that you are not removing any important controls. Merging multiple similar controls is typically done using the "strongest" formulation / point. The one control which has the strongest or the most comprehensive statement wins. But aggregation can be done in different ways which we will discuss now.

## New Catalogue

# Catalogues

Remove duplicates

Aggregated catalogue

22

For this type of aggregation we take all the relevant authority documents. We remove duplicates and create a new catalogue. We do not take care about formulation and which authority document has the most comprehensive statement.

This is why that type of aggregation makes most sense with authority documents that have no intersection.

## Master Catalogue

#### Master Catalogue



Aggregated catalogue

23

With this type of aggregation one authority document is defined as the master catalogue. All controls from that authority document are taken and are supplemented by controls from the other authority documents.

It is important to note that the master catalogue is always "winning" against the other authority documents. If the master catalogue and another authority document contain a control which is about the same thing, then we take the control from the master catalogue. It does not matter if the master catalogue contains the strongest formulation or not.

# Weighting

#### Catalogues

Remove duplicates, weighting

Aggregated catalogue

24

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

25

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.

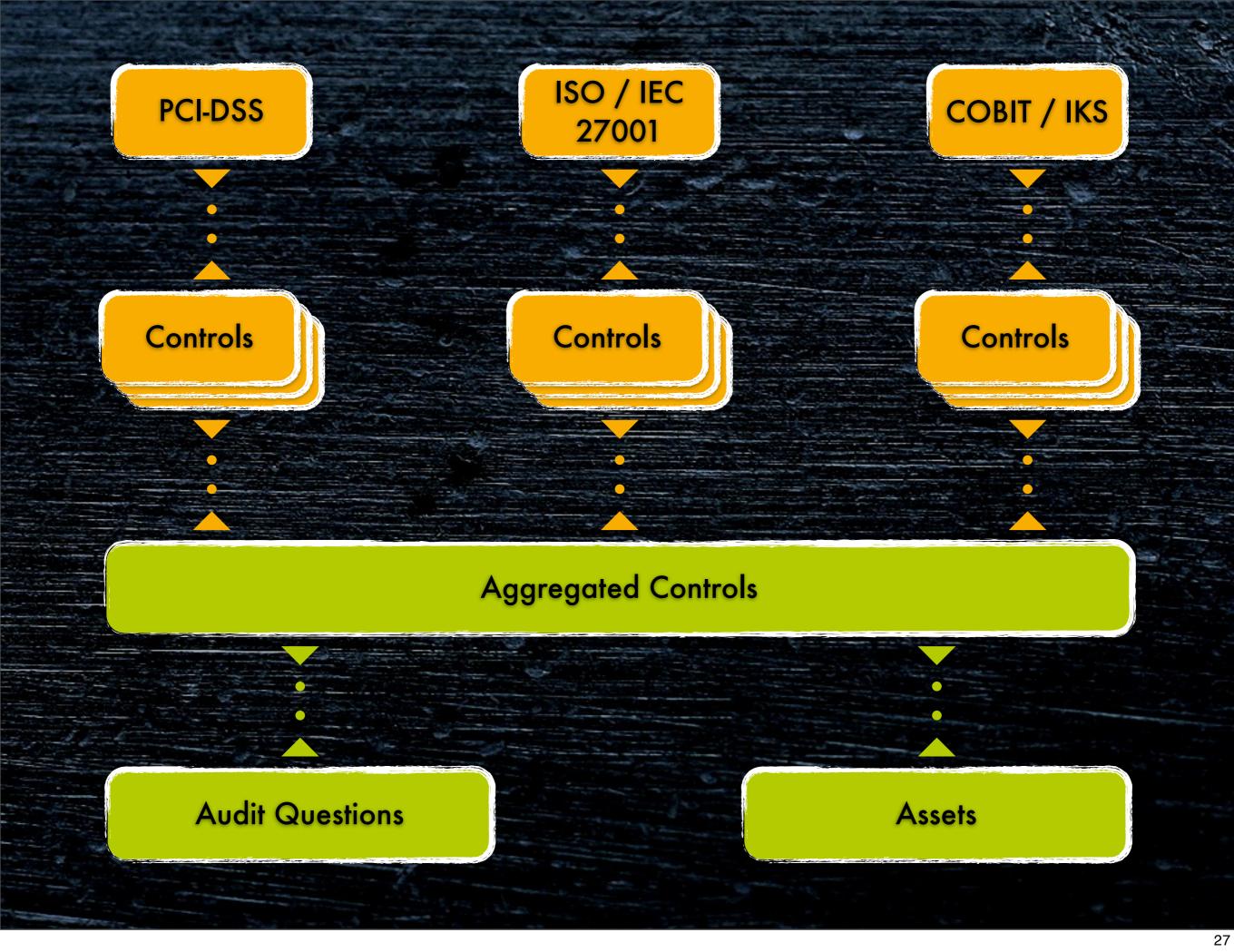
It is very important to note here, that even when you go and buy that UCF, you will always have to work yourself through the whole set of controls. The UCF is not a catalogue of its own but an intelligent manning information. But at least you have some guidenes and

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

The second strategy is the self assessment. We will now talk about that strategy.

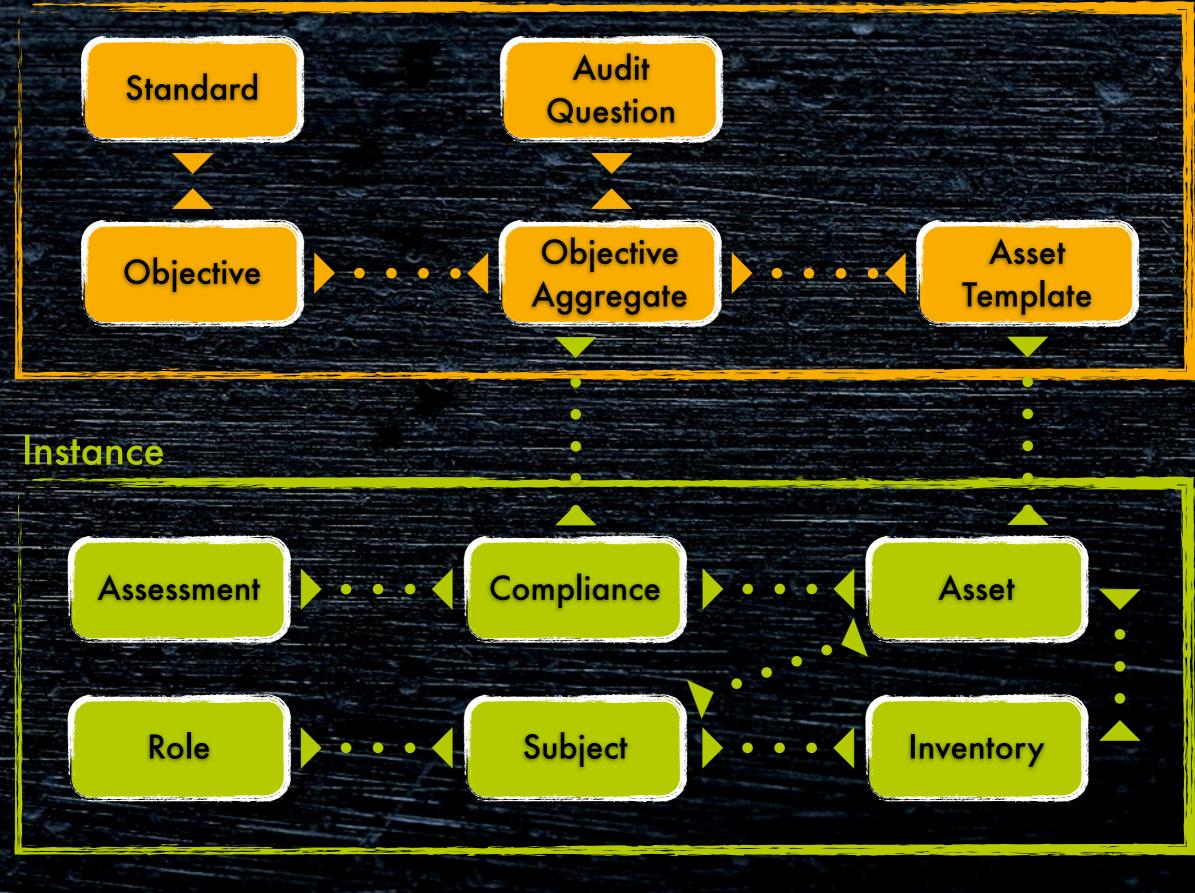


For the self assessment, the aggregated controls are linked with audit questions and assets. With these links we can automatically determine which audit question is relevant for which control for which asset type.

# Strategy #3 Meta Data Model

And the third strategy is a powerful meta data model.

Model



Our data model is basically grouped into two groups: Model and Instance.

#### Model

Similar to the concept of classes and instances in computer programming our model part is some kind of template or instruction manual. The model part contains the authority documents (standard, objective), the aggregates (objective aggregate), audit questions and the reference to asset templates.

Using such model it is possible to define which controls are relevant for what types of assets.

29

The whole database model is also working with UUIDs as primary keys. Because of that it is possible to share that model part of the database amongst several parties. The model part does not differ between parties because it does not contain any data from a specific environment. It only contains meta data describing how asset templates link to controls.

#### Instance

The instance part contains all instances and environment specific data. It does contain users and responsibilities (subject, role). it does contain a copy from an inventory (copied with the help of an ETL tool from an existing asset management database). And this part also contains all the assessment specific data. Which is the assessment, all assets in scope and the answers to the audit questions (compliance).

Which means it is possible to have multiple assessments without the need to change anything in the model part or somewhere else. As long as the authority documents do not change.

Some other points to consider:

- Also instances use UUID. So road warriors could work on the road and afterwards synchronise with the main database.

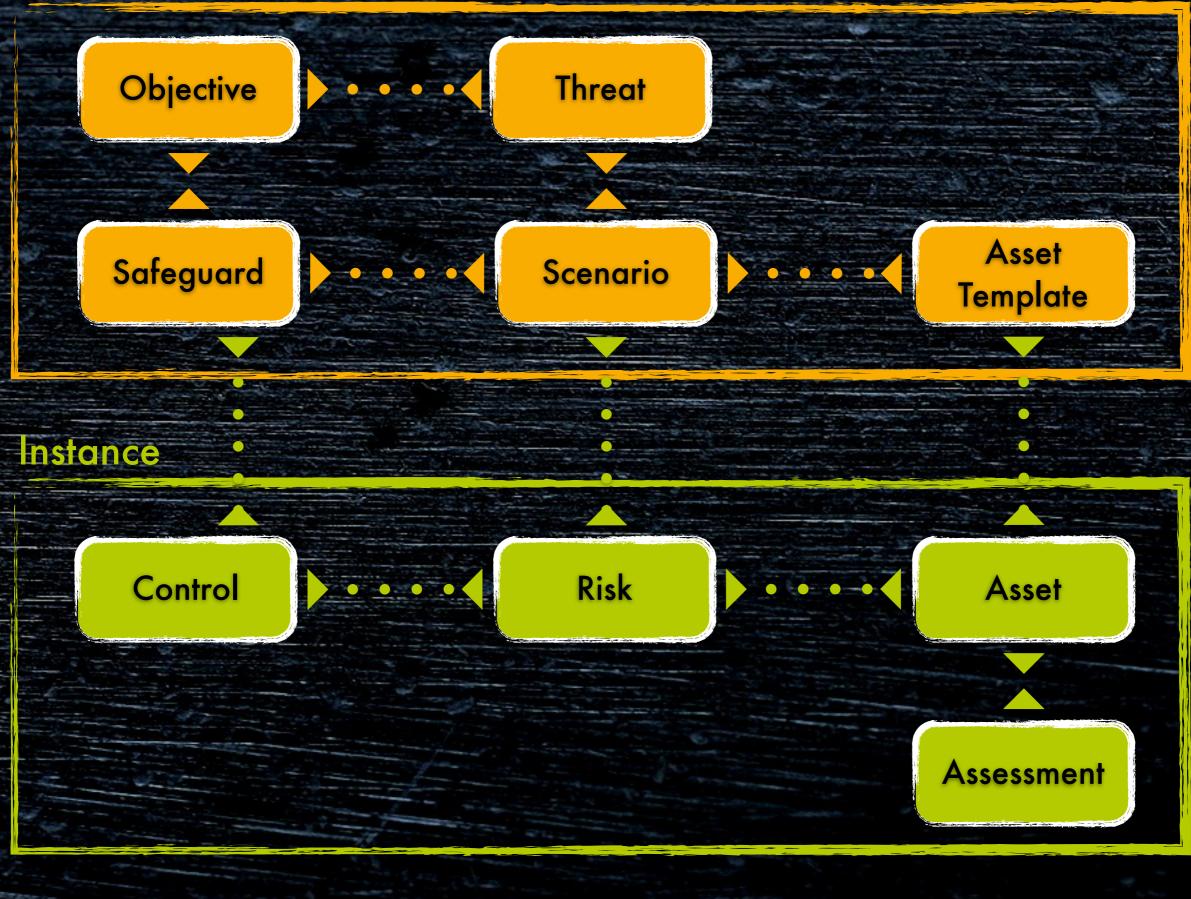
- Assessments can be linked with each other, giving the possibility for historical reports and analysis.

# Strategy #4 Reuse the Meta

### ...for Risk Assessments



Model





# Strategy #5 Don't do silly calculations

# Strictly no silliness

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

A.FORC

Now that we talked about what we do today, let's have a look at what could be cool in the future.

### Metrics

Contexts	Search Results	strong-auth-coverage
Security Discipline     Public Data Source Metrics     PCI DSS v1.2     Source 1. Build and Maintain a Secure Network     C. Protect Cardholder Data	Advanced Search	Name:       strong-auth       Version:       0.1*       Item         Owner:       6AC5:eJyz4F       Group Owner:      public         Rating:       Views:       41
<ul> <li>3. Maintain a Vulnerability Management Progra</li> <li>4. Implement Strong Access Control Measures</li> <li>5. Regularly Monitor and Test Networks</li> <li>6. Meaintain an Information Security Policy</li> <li>NIST Metric Type</li> </ul>	- Popularity - Full Text Serach	Created: 2009-01-25 Updated: 2011-09-19 Title: strong-auth-coverage Status: Draft Units of Measure: Percentage of Critical Assets
NIST SP800-53 Controls     SO/IEC 27002	Clear Search	Targets: 100%
<ul> <li>0. Introduction</li> <li>1. Scope</li> <li>2. Terms and Definitions</li> <li>3. Structure of the Standard</li> <li>4. Risk Assessment</li> <li>5. Security Policy</li> <li>6. Organization of Information Security</li> <li>7. Asset Management</li> <li>8. Human Resources Security</li> <li>9. Physical and Environmental Security</li> <li>10. Communication and Operations Management</li> </ul>		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
<ul> <li>I1. Access Control</li> <li>I1.1 Business requirement for access contro</li> <li>I1.2 User access management</li> <li>I1.3 User responsibilities</li> </ul>	passwords that are set to expire in accordance with policy. 11/06/2011(0.1*)  strong-auth-coverage This metric measures the percentage of systems	fingerprint). Therefore, an example of strong authentication would be a password (something you know: factor #1 and a fingerprint (something you are: factor #2).
<ul> <li>11.4 Network access control</li> <li>11.5 Operating system access control</li> <li>11.6 Application and information access con</li> <li>11.7 Mobile computing and teleworking</li> </ul>	with critical information assets that use stronger authentication than IDs and passwords in accordance 10/27/2011(0.1*) accounts-closed-correctly	Objective: This baseline metric measures the extent to which authentication that is stronger than one-factor authentication has been implemented for critical assets.

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 to data to answer it for yourself.

36

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 manyfold: 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