

### Build yourself a risk assessment tool

**The plan**: 25 min theory 20 min practice 5 min questions

#### Vlado Luknar

CISSP, CISM, CISA, CSSLP, BSI ISO 27001 Lead Implementer di-sec.com

### Do you need your own tool?



- **short answer** maybe *not* if you're happy with what existing methodologies & tools offer
- **long answer** maybe *you do* if you're left alone with it and don't know where to start and feel like you might want to have more freedom

### disadvantages of ready-made tools

- (many) single user, single assessment case, not integrated
- those sophisticated ones, based on web, for multiple users – may be expensive, suited for full-time experts (OCTAVE, Proteus)
- those coded in java or using desktop db runtimes very much static
  - you might depend on provider for any design and maybe also content changes

### Advantage of own, custom-made tool

you have the full control over

- the **functionality** and
- the **content**
- you can truly shape the tool around your own needs

it can become more than just a risk tool:

- it can be part of an overall ISMS
- combining all internal knowledge about status of

- information security in your company

if created with accessible technologies (HTML, CSS, javascript, PHP)

- chances are you will not get stuck with it
- never obsolete since everything is under your nose

### What this presentation is not about

breakthrough in information security risk assessment (RA)

- it is not about **rightfulness** of any methodology
- there are tons of **scientific papers** to read
- unfortunately, what one can do with them is **quite limited** although research is very **interesting**
- it is of little help when doing RA in a real company, e.g.
  - if you cannot agree who is responsible for an asset...
  - or, who has to approve the access..

the real everyday security struggle is rather different from books

- it takes place in your own, specific company
  - with different set of conditions, limitations and skill-sets

### What this presentation is about

there is no problem with understanding methodologies, yet

- it is really not that easy to start with any of them
- there is no single best approach to RA for everyone

#### for RA to be practical we need to

• simplify things as much as we can

#### the pragmatic approach is the one

- which is good-enough, meaning
  - quick can be performed by **non-RA specialists**
  - focuses only on what really makes-or-breaks the security in a given case
  - repeatable, reproducible and stable over time

## The journey or the results?



exaggerating a little we could say the real purpose of the RA

• is not the **result** but the **journey** itself

the journey during which we learn what didn't know:

- about our environment (people, process, technology)
- that instead of relying on few key assumptions, like
  - people are following standards and procedures, or
  - vendors are **patching** our systems
  - sometimes it is worth investigating deeper
- by repeating the process, performing RA consistently
  - we learn which security measures make sense
  - which to embed into ISMS and which keep out for specific cases

# Setting the ground



a risk assessment can be performed at several levels of details

- **business** (high) to map business or organizational risks
- **process** (medium) compliance with best practices or international standards for info security management
- **technical** (low) aiming at **threat modeling** (such as STRIDE) some opinion-making methodologies (NIST SP 800-30)
  - assume that the technical level deals both **process** and **technical** risks (selecting technical controls, setting actions)

when we need to stick to known compliance frameworks, such as

- ISO/IEC 27001, COBIT, PCI DSS or SOX
- most likely we end up working with **people**, **process** and **technical** risks

### List of best known tools

### For those still looking for the ultimate tool

 COBRA, CORAS, CRAMM, EBIOS, FAIR, FRAP, GSTool, MEHARI, CORA, ISACA COBIT 5, ISRAM, ISF IRAM, MAGERIT-PILAR, OCTAVE, Proteus Enterprise, RiskSafe, RiskWatch, Verinice

### In 2014 Gartner compared the following methodologies/tools:

• FAIR, ISACA COBIT 5, ISF IRAM, ISO/IEC 31000:2009, MAGERIT, NIST SP 800-30, OCTAVE Allegro, and RiskSafe by Platinum Squared Technologies (which is a SaaS-based approach)

Gartner's summary:

• "choose the risk assessment methods that are the **best cultural fit** for your organization."

## Key definitions



# despite all that scholars know about **risk** it remains a **vague** and somewhat **confusing** concept.

- "Prediction is very difficult, especially about the future." Niels Bohr
- "The idea that the future is unpredictable is undermined every day by the ease with which the past is explained." Daniel Kahneman

#### most of our past experience (incidents, checks, audits) demonstrates that

- even the simplest assumptions in RA can be wrong
- the expected (routine) controls and measures are ineffective or inefficient
- a RA is about best collective judgment
  - "Managing information security risk, like risk management in general, is not an exact science. It brings together the best collective judgments of individuals and groups within organization." (NIST SP 800-39)

### What we need to build our tool



### approach - we might follow a known methodology

• ISO 27001 is considered a **top-down**, **technology-neutral** 

- most people know it, we can compare and benchmark against others completely own risk methodology - should have a reason

### minimal functionality

- catalogue of assets
- catalogue of threats
- vulnerabilities linked to threats
- controls linked to vulnerabilities

#### nice-to-have features

- list of risks with linked RTPs
- live repository of **security references** (policies, procedures)
- incidents and audits stats
- reporting, charts, exports

## Sources of information on TVCs 1/3



#### Books

• Information Security Risk Assessment Toolkit, Practical Assessments through Data Collection and Data Analysis M.R.M.Talabis, J.L.Martin, 2013 Elsevier

### Source of assets

- your own (automated) inventory system
- business architecture systems (such as ARIS-BP)

### Source of threats

OSA compared threat catalogues in 2008 (http://opensecurityarchitecture.org)

- BITS Kalculator (600 Ts), ISF IRAM (39 Ts), NIST SP 800-30
- BSI (Bundesamt für Sicherheit in der Informationstechnik) (370 Ts), ISO 27005 (43 Ts)
- **simplicable.com** The Big List of Information Security Threats, John Spacey, Simplicable, December 08, 2012

### Sources of information on TVCs 2/3



#### Source of vulnerabilities

- some good generic examples which can be adapted or expanded from are
  - ISO 27005
  - Information Security Forum (ISF IRAM tool)
  - NIST SP 800-53
- other (internal) sources
  - vulnerability assessments, penetration testing, audit reports, security incidents
- maybe one can get **inspired** also by technical vulnerabilities as maintained via CVE (MITRE, DHS U.S.)
  - http://web.nvd.nist.gov/view/vuln/search-results?query=authorization
     +bypass&search\_type=all&cves=on

### Sources of information on TVCs 2/3



#### Source of controls

- ISO 27002 (114 Cs), BITS (219 Cs)
- NIST SP 800-53 r4 (163 Cs)
  - catalog of security and privacy controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations
  - NIST say the controls are intentionally technology-neutral and policyneutral
- OSA http://www.opensecurityarchitecture.org/cms/library/0802control-catalogue
- OWASP
  - (web) application controls (11 subcategories, 45 controls)
  - OWASP ISO/IEC 27034 Application Security Controls Project (only starting)

### Which open-source to use?

#### any one that is really open

- source code made available with a license in which the copyright holder provides the rights to study, change and distribute the software to anyone and for any purpose
- allowing to see how things are done from inside and
  - not limiting what you can do with your own data
- supports scripting, public repositories and rapid deployment
- has a huge installed base (with forums, groups)
- mastering it does not require a MIT degree

two of many possible directions for a home-made risk tool

- a wiki variant (twiki, dokuwiki, mediawiki, tiddlywiki)
- CMS system (Drupal, Joomla, Alfresco, ocportal, tiki)

# Why tiddlywiki?



"the simplest online database that could possibly work" Ward Cunningham (on **wiki** concept)

- free, low footprint and easy **operability**
- user needs only a web browser and a username (to sign posts or to login where needed)

dynamics of data from the **user side**:

• end-user himself creates logical relationships between pieces of data the way he/she wants it

#### all done from within a web browser

- no need to work with database schemas, entities, relationships
- records can contain other records or even scripts

### About the live demo of the tool

#### one important question is

- how much **automated calculation** do we want in the tool?
- even the most **sophisticated formulas** do not make risk calculation "better"
- because the key is knowledge of
  - context, make-or-break points,
  - history: incidents, findings, and actual status of controls

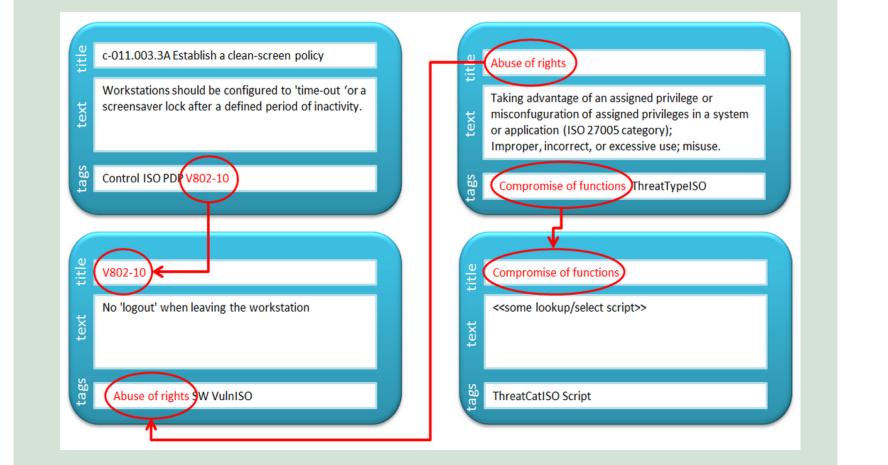
my experience (e.g. with IRAM tool by ISF, done in Excel)

- if everything is auto calculated
- w/o possibility of a (collective) human verdict
- people tend to "play" with the tool until the issues "disappear"

the live demo is an experimental version of the tool, a mix of (mostly) real and (some) random data

### The "engine" behind





### RISSCON - printscreens 1/3



Target Objectives Context Index Impact TVC Risk ra	ating (manual) Risk rating (calculated) Summary
Threats Vulnerabilities Controls	
show/hide	
Overall criticality of assets 🗸 data 🗌 hardware 🗌 software 🗌 sites 🗌 staff int	ternal 🗹 3rd party
Overall criticality of architecture 🗸 web 🗌 database 🗌 cryptography 🗌 cloud	virtualisation
Compromise of information	Natural events
Data from unreliable or untrusty sources	Climatic phenomenon
<b>Oisclosure</b>	Flood
🗹 Eavesdropping	Meteorological phenomenon
Interception of compromising interference signals	s 📄 Seismic phenomenon
Position detection	Volcanic phenomenon
Remote spying	
Retrieval of recycled or discarded media	Division demons
🔽 Tampering with hardware	Physical damage
Tampering with software	Destruction of equipment or media
Theft of equipment	Dust, corrosion, freezing
Theft of media or documents	Fire
	Major accident
	Pollution

### RISSCON - printscreens 2/3



arget	Objectives         Context         Index         Impact         TVC         Risk rating (manual)         Risk rating (calculated)         Summary
Threat	Vulnerabilities Controls
Asset	Architecture view
Assets 1	ighlighted: 🗹 💷 data 🗔 🖄 hardware 📄 亘 software 📄 💁 sites 📄 😃 staff internal 🍼 🗟 3rd party
	sment: <sup>(1)</sup> selected <sup>(2)</sup> assigned to this RA
Threat	✓ Abuse of rights
• Thi	threat could exploit the following vulnerabilities:
0	🗸 💼 📄 🐵 🗆 🖾 🗸 🗖 📄 🖍 🖳 🔛 V802-9 Flaws in software affecting authentication and authorisation
0	🗸 🍘 📄 🐵 📄 🔛 🔀 🗸 🗖 📄 🔝 🔛 🔛 V802-8 No or insufficient software testing
	🗸 🌐 🗌 🗐 🔚 🔀 📄 🗖 🗖 🖳 😫 🖓 V802-7 Lack of fault reports recorded in administrator and operator logs
٥	V - V V V V V V V V V V V V V V V V V V
	Image: Second decision of the second
0	<ul> <li>Image: Second sec</li></ul>
0 0	Image: Constraint of the system of the sy
0 0	<ul> <li>Image: Second sec</li></ul>
0 0 0	Image: Constraint of the system of the sy

### RISSCON - printscreens 3/3



Target         Objectives         Context         Index         Impact         TVC         Risk rating (manual)         Risk rating (calculated)         Summary
Threats Vulnerabilities Controls
All managed controls Only scope controls
Exposure Controls in detail
Threat:  Abuse of rights
Exploitable vulnerabilities:
• ✓ finally selected saved with this RA V802-9: Flaws in software affecting authentication and authorisation
Vulnerability is rated: Medium
● ✔ finally selected saved with this RA V802-8:No or insufficient software testing
Vulnerability is rated: Low
•      ✓      finally selected □ saved with this RA V802-7:Lack of fault reports recorded in administrator and operator logs
Vulnerability is rated: High
• ✓ finally selected □saved with this RA V802-6:Lack of procedures of risk identification and assessment
Vulnerability is rated: Medium

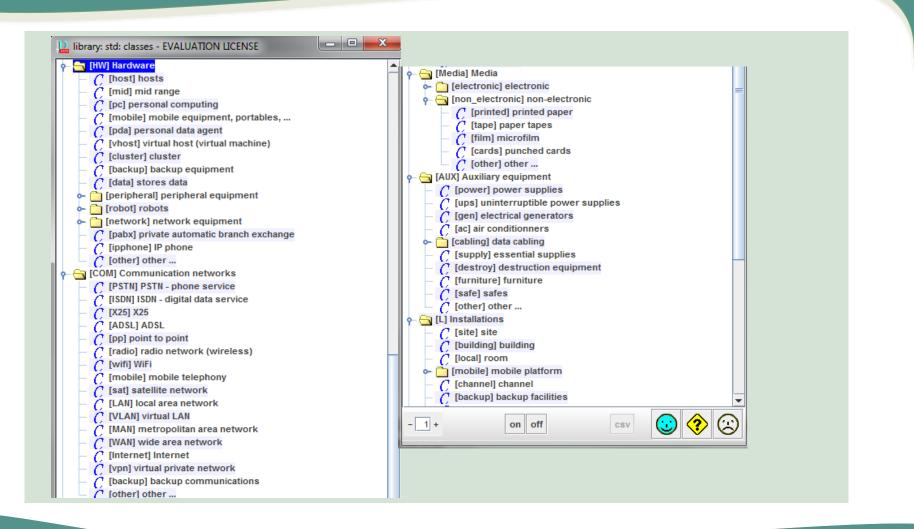
### GSTOO (Bundesamt für Sicherheit in der Informationstechnik, Ger)



New		(indow <u>H</u> elp	ă 🗸	F5 fresh		Filter	Model	View	Catalogs I	ocal Catalogs o	nline N	lavigator
Structure of rget objects	ojectmodel:BSI ☐ BSI — • • • Universally ( — • • • • • • • • • • • • • • • • • • •	applicable aspe T Security Mana		Co <u>m</u> Cata	log:	(All)	uards   Th <u>r</u> eats	Notepad				
Modeling	⊕ M1.2F     ⊕ M1.3C     ⊕ M1.4C     ⊕ M1.4C     ⊕ M1.5C	Organisation Personnel Contingency Pla Data Backup Po Data protection / Concept of comp	licy		No. S 2.110 S 7.1 S 7.2 S 7.3	Data protect Specificatior	on guidelines for ion management i of the responsib data protection c	ilities for data pr		Catalog Organisation Data protection Data protection Data protection	Security - - -	seal lev P 1 3 2 1
isk analysis Reports		Crypto-concept Handling of secu Hardware- and S Standard softwi Outsourcing Archiving	rity incidents Software-Manageme		S 7.4 S 7.5 S 7.6 S 7.7 S 7.8 S 7.9	Definition of t Obligation/b Organisatior Maintaining a Data protect		ational measure mbers for the pro r protecting the r ers and complia	is accordin pocessing of ights of dat nce with co	Data protection Data protection Data protection Data protection Data protection Data protection	- - -	1 1 1 1 3
-Grundschu user defin €					S 7.10 S 7.11 S 7.12 S 7.13 S 7.14 S 7.15	Regulation of Regulation of Documentati Maintenance	ind specification f commissioned f linkage and use on of admissibilit e of data protectic struction in compli	data processing age of data rega y regarding data on during operati	regarding t rding the pr a protection on	Data protection Data protection Data protection Data protection Data protection Data protection	-	1 1 5 1 1
-Grundschu manage Export/	4			•			III		Reve	rt Dele	ete	<u>N</u> ew

### Magerit-Pilar (National Intelligence Centre, Spain)





### NIST SP 800-53



TABLE D-2: SECURITY CONTROL BASELINES <sup>92</sup>											
CNTL			INITIAL CONTROL BASELINES								
NO.	CONTROL NAME	PRIORITY	LOW	MOD	HIGH						
Access Control											
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1						
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)						
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3						
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4						
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5						
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)						
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7						
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8						
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected						
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10						
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)						
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12						

#### 92