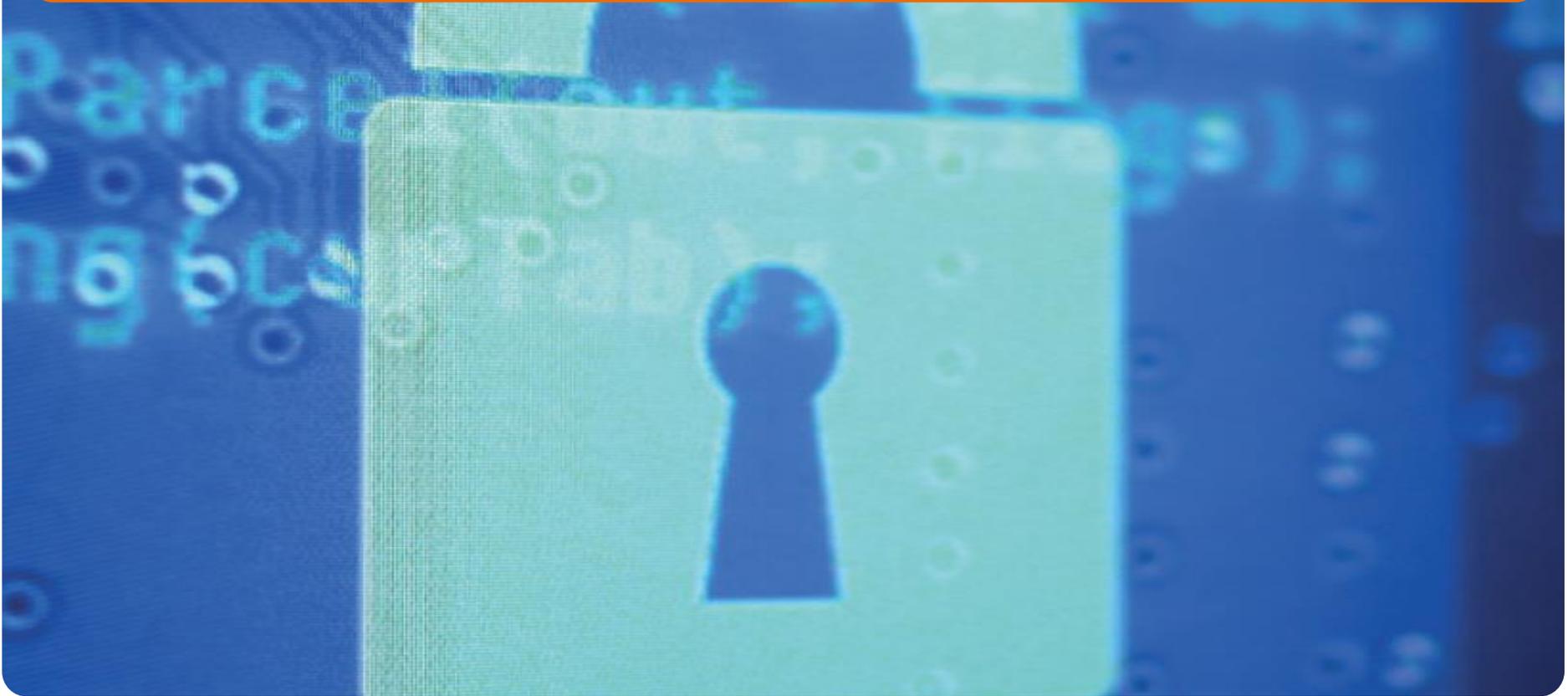


Tools and tips for secure assessment



Annette Peet

13 april 2018

SURF



AGENDA

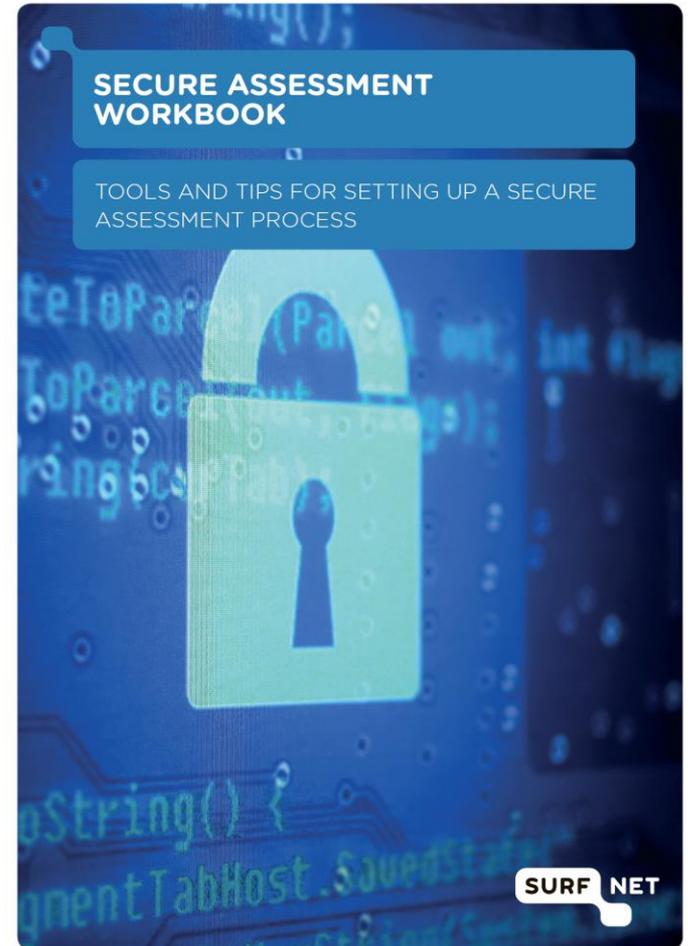
- Introduction
- Secure assessment workbook:
 - Why?
 - For whom?
 - Scope
 - Approach
 - Tools & checklists
 - 5 steps
- Awareness
 - Examples from NHTV, Saxion and TU/e

Some questions....

Please go to: [menti.com](https://www.menti.com) and use code:
411577

Secure assessment workbook in a nutshell

- Why?
- For whom?
- Scope
- Approach
- Tools & checklists
- 5 steps



Why?

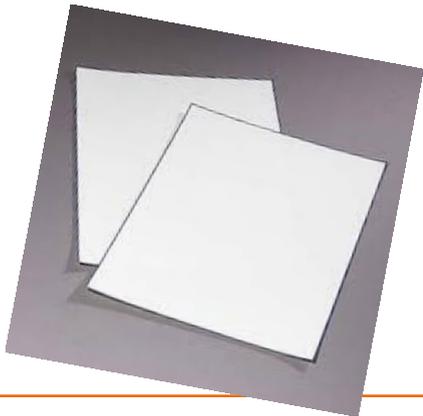
- Growing awareness of the importance of a secure (more secure) assessment proces – partly due to the growth of digital assessment
- Complexity of the assessment process
- Joined forces of several institutes:
 - **Amsterdam University & University of applied science**
 - Delft University of technology
 - **Eindhoven University of technology**
 - **Groningen University**
 - Hanze University of applied science
 - Inholland University of applied science
 - Maastricht University
 - **Saxion University of applied science**
 - **The Hague University of applied science**
 - Windesheim university of applied science

For whom?

- Employees in higher education institutions involved in secure assessment:

...employees of the assessment office, assessment software administrators and security officers (CISOs)...

SCOPE



Discussion



What is
'secure
assessment'?

Start with the basics: baseline information security

- The institution complies with *the higher education information security **Baseline*** (jointly defined)
- Full implementation delivers a generic information security at a medium level
- The workbook helps you define the extra security measures for secure assessment



Workbook: Tools & checklists to help you

APPENDIX 1

Detailed example of the assessment process

APPENDIX 2

Secure assessment based on information security baseline

APPENDIX 3

Security measures for each sub-process

APPENDIX 4

Secure assessments review

APPENDIX 5

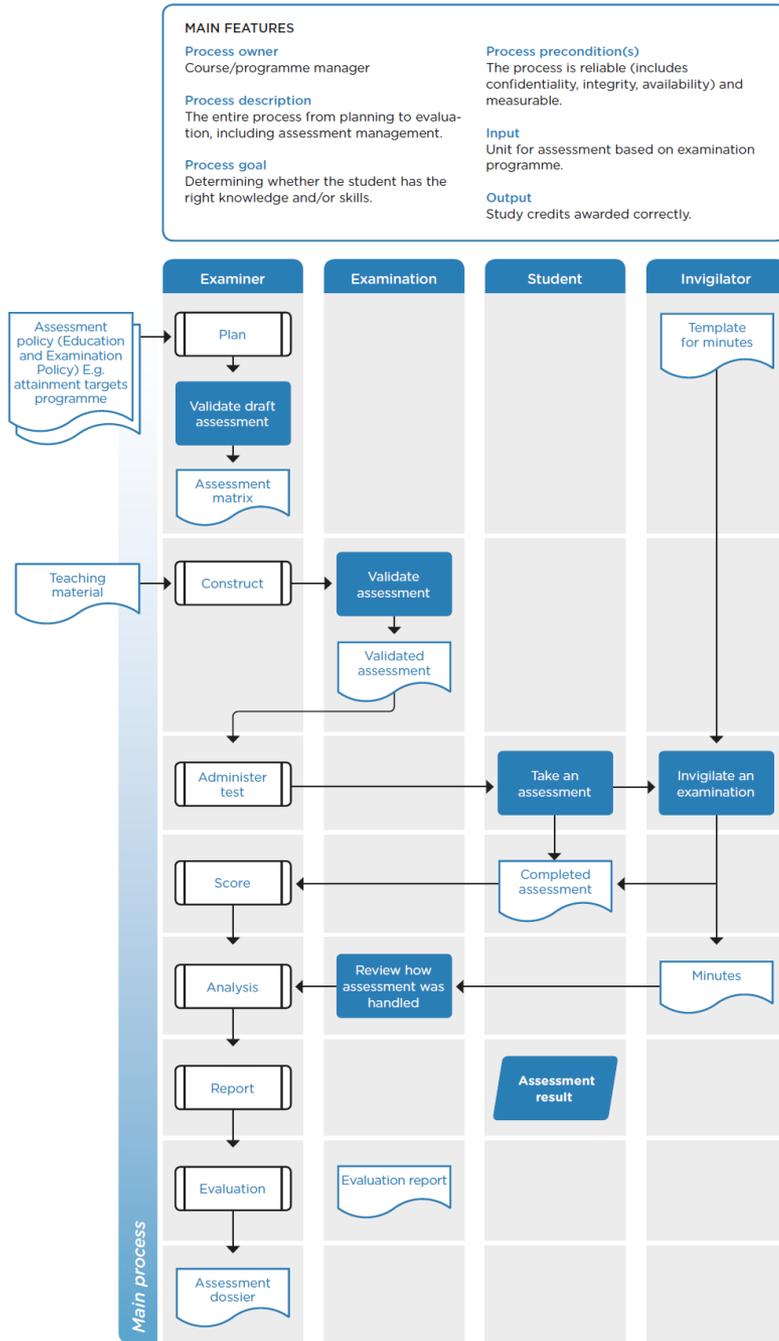
HORA objects falling within the test process

APPENDIX 6

Source material used

SECURE ASSESSMENT CHAIN

PROCESS MODEL



SUB-PROCESS 4

SCORING

MAIN FEATURES

Process owner
Examiner

Process description

Scoring the completed questions and assigning a provisional grade to answers, in line with the standard.

Process goal

Give completed assessment a grade as required

Process precondition(s)

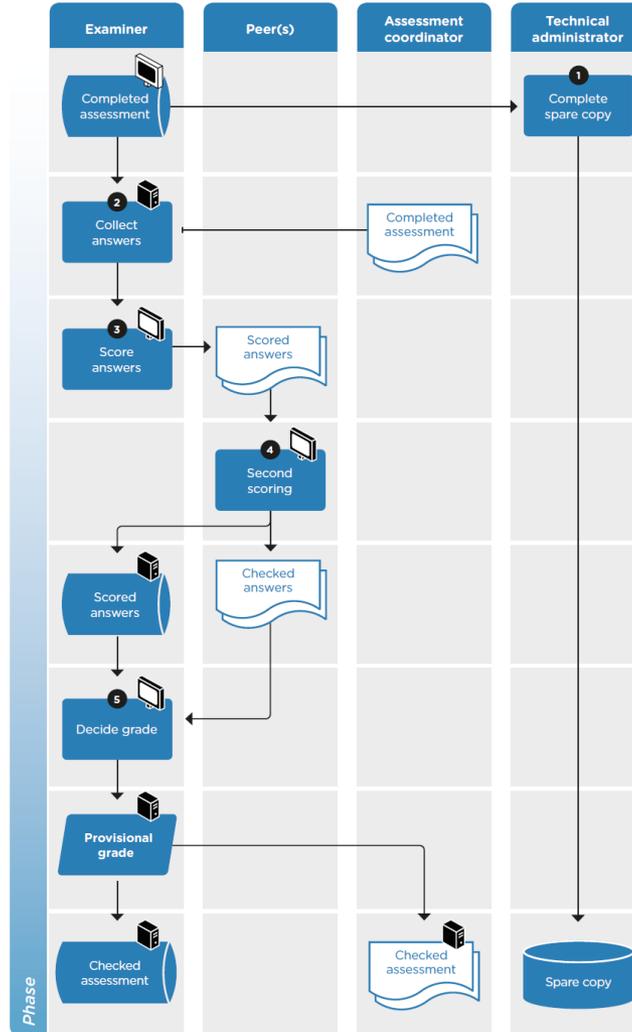
Process is reliable (includes confidentiality, integrity, availability) and measurable.

Input

(Template) Answers to the assessment standardisation (e.g. rubric)

Output

Graded assessments (provisional results), verified standardisation



ACTIVITIES IN SUB-PROCESS 4: SCORING

	Activity	How (procedural description)	When	Who
1	CREATE BACKUP	Directly after the completion of a digital examination session, a spare copy of the completed tests is made.	Within one hour after the end of the assessment	Software administrator
2	COLLECT ANSWERS	The examiner collects the completed assessments. For multiple choice assessments taken digitally, this may mean collecting a CSV file containing answers, gaining access to the item bank where the completed assessments are held or collecting a set of papers.		Examiner
3	SCORE ANSWERS	Compare the answers with the standard answers. This is either done in full by the examiner or supported by the assessment programme if it is a partial or complete digital assessment.		Assessment coordinator
4	SECOND SCORER	If the detailed rules of the assessment require this, the assessment is scored by a second corrector.		Peer(s)
5	DETERMINE GRADE	The examiner assigns a provisional grade to the completed work.	Within one week of the assessment	Examiner

1.1. Plan

Like many other business processes, planning assessments has become digitalised over the years. Assessment planning has not fundamentally changed due to the advent of digital assessments. Planning takes place mainly under the direct control of the examiner, within his/her own organisational unit.

Activity	Integrity and confidentiality risks			Management measures				
		Opportunity	Impact		setting up a system	authorisation (separation of duties)	reports	user controls
			I	C				
1. Define assessment structure		-	-	-				
2. Define assessment matrix	Unauthorised access to the examiner's workstation	M	L	L				
	Interception of the assessment matrix during transfer between the workstations of those involved	L	L	L				
	Unauthorised access to the shared environment	M	L	L				
3. Review assessment matrix	Unauthorised access to the assessment expert's workstation	M	M	L				
4. Process feedback on assessment matrix	Feedback not received	M	H	L	Automatic version counter	Only identified persons have the right to update		Examiner notifies peer that feedback has been processed
	Feedback not processed	L	H	L			Access log Update log	Regular access and version check by assessment coordinator

1.2. Construction

The assessment questions (assessment items) are developed during the creation of the assessment. Because assessment questions for summative assessments may never be known in advance by the students, there is a significant risk involved. The table sets this out in detail. In this part of the assessment process, a number of risks recur several times. As in some cases other management measures may be needed, they cannot by definition be resolved in one go for various activities.

Activity	Integrity and confidentiality risks			Management measures				
		Opportunity	Impact		setting up a system	authorisation (separation of duties)	reports	user controls
			I	C				
1. Define assessment items	Unauthorised access to the examiner's workstation	M	L	H	Local storage only if encrypted, or storage in a (private) cloud	Access to PC with personal account only	Audit trail after upload with user and date/time	Regular monitoring of login behaviour
	Unauthorised access to the author's environment (software, data)	M	L	H	With two-factor authentication and encrypted connection	<ul style="list-style-type: none"> Establishment of need-to-know access Personal login 	Audit trail with user and date/time	Regular monitoring of login behaviour
2. Review assessment items	Interception of assessment items during transfer from examiner's workstation to shared environment	L	M	H	Data sent in encrypted format	<ul style="list-style-type: none"> Only required persons are granted read- and write-access Previous versions cannot be overwritten 	Track changes, keep previous version(s)	Notification of changes to relevant persons
3. Process feedback	Unauthorised access to the examiner's workstation	M	M	H	Local storage only if encrypted, or storage in a (private) cloud	Only assessment owner (examiner) has rights to accept track changes.	<ul style="list-style-type: none"> Track changes are visible Response to review is defined 	Notification when track changes are processed

Five steps towards a secure assessment proces

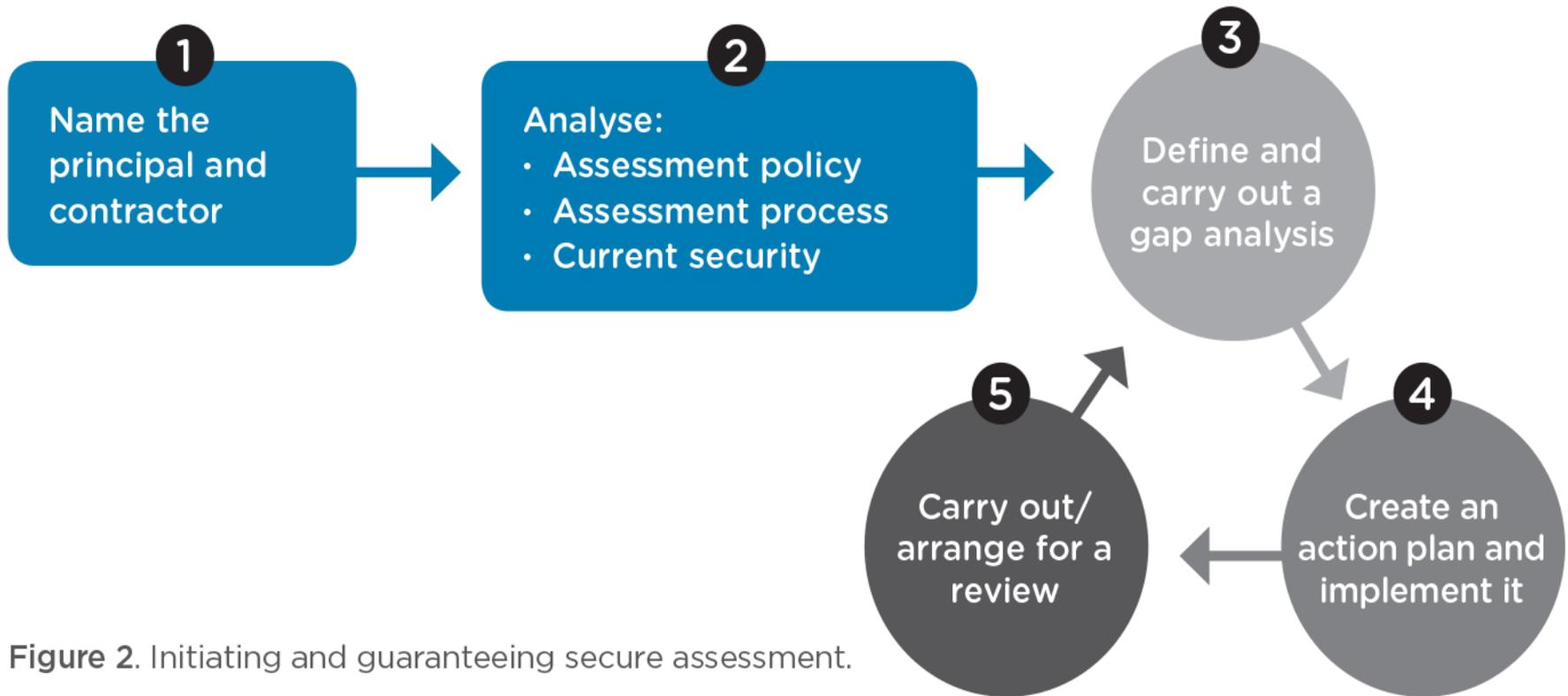


Figure 2. Initiating and guaranteeing secure assessment.

How to create awareness for security?

1. How to create awareness for security?
2. Who are key players?
 - *Who's should be the principal (assignor)?*
 - *Who's could be the executant?*
 - *Who else do you need?*

Awareness @NHTV



Campagne van Saxion

1. Één voor allen

https://video.saxion.nl/media/01+E%C3%A9n+voor+allen/1_2gn37oj1

2. Plagiaat Magnaat

https://video.saxion.nl/media/02+Plagiaat+Magnaas/1_tre0iu5c

3. Multiple Choice

https://video.saxion.nl/media/03+Multiple+Choice/1_ljbxqi84

4. Saxion Gate

https://video.saxion.nl/media/04+Saxion+Gate/1_hg3fqngr

Klaar voor je tentamens?

Ook dit hoort erbij! /

Ready for your exams?

This also comes into it!



Campuskaart
Campuscard



Kom op tijd
Be on time



Apparatuur uit en in gesloten tas
Switch off devices and in a closed bag

Thank you!



Annette Peet
Project manager
SURFnet

annette.peet@surfnet.nl