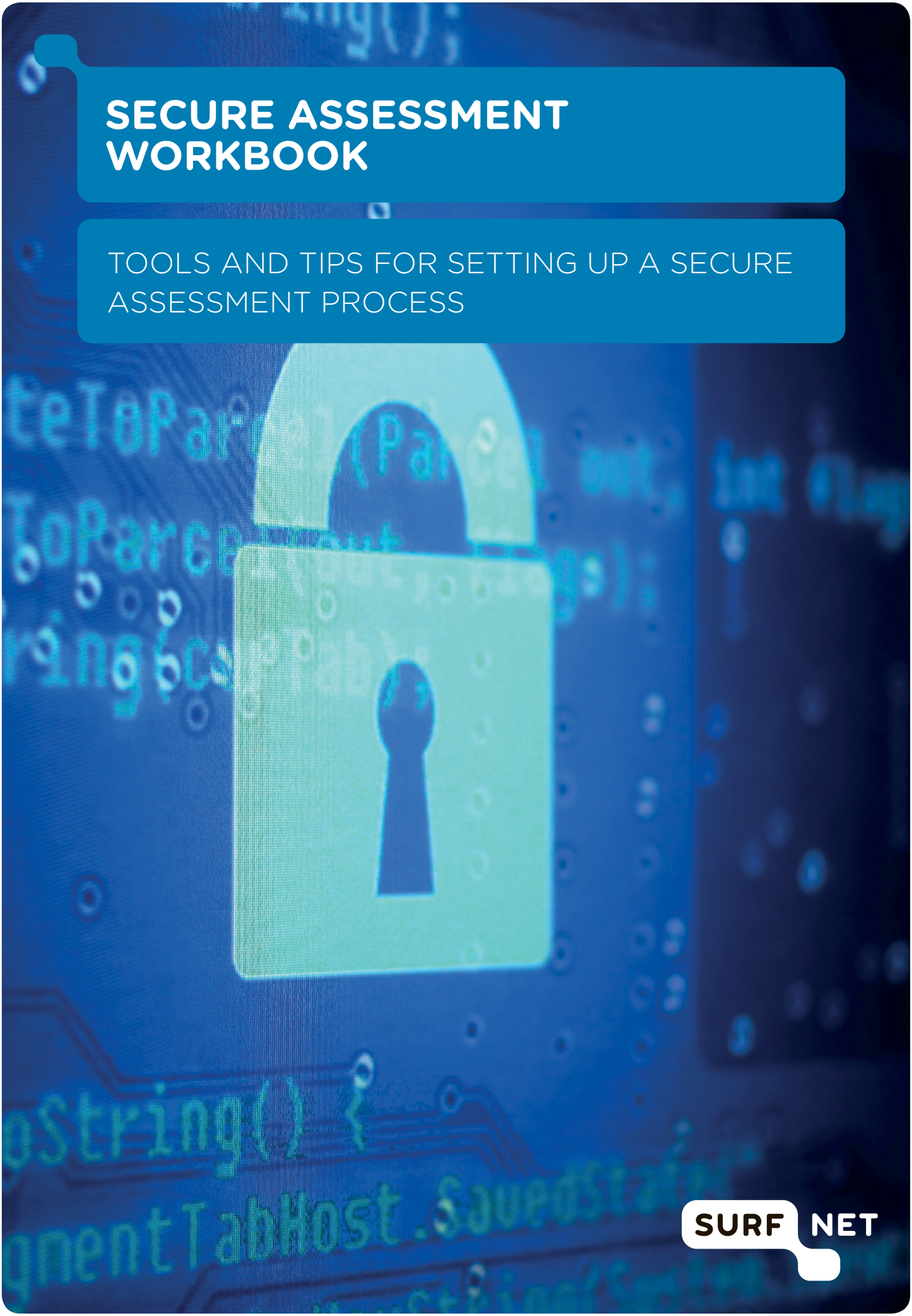
# SECURE ASSESSMENT WORKBOOK

TOOLS AND TIPS FOR SETTING UP A SECURE ASSESSMENT PROCESS



SURF NET

# TABLE OF CONTENTS


1. INTRODUCTION 5
   1.1. Who should read this 5
   1.2. Scope: digital and paper assessment 5
   1.3. Responsibility 6

INTERMEZZO
Examples of assessment in practice: risks and points to look out for 7

2. SECURITY RISKS IN THE ASSESSMENT PROCESS 10
   2.1. Risk analysis 10
   2.2. Success factors for secure solutions 12

3. TOWARDS A SECURE ASSESSMENT PROCESS 13
   3.1. Overview of stages 13
   3.2. Stage 1: Task and ownership 13
   3.3. Stage 2: Analysis of current situation 14
   3.4. Stage 3: Gap analysis 14
   3.5. Stage 4: Action plan for secure assessment 14
   3.6. Stage 5: Review 14
   3.7. Future-proofing secure assessment 14

4. CONCLUSION 15

APPENDICES 16
Appendix 1 Detailed example of the assessment process 17
Appendix 2 Assessment security on the basis of baseline information security 43
Appendix 3 Security measures for each sub-process 45
Appendix 4 Review of secure assessment 62
Appendix 5 HORA objects falling within the test process 64
Appendix 6 Source material used 65

# 1 INTRODUCTION

With the advances in digital assessment, institutions are more aware that the security of the assessment process is becoming ever more important. The need for secure assessment goes beyond digital assessment alone, if only because lecturers generally make use of IT when preparing paper-based tests too. Securing the assessment process is not simple; there are unfortunately no comprehensive measures which can solve everything in one go. In order to support institutions in making the assessment process secure, SURFnet has been working with experts from various institutions of higher education to develop this workbook. Where the text says "we", this core group is what it is referring to.

## 1.1. Who should read this

This workbook offers institutions guidance on setting up the complete assessment process securely. This guidance is in accordance with existing relevant security guidelines and standards as far as possible. It provides an overview of practical measures that can increase security.

It is intended for employees in higher education institutions who are involved in secure assessment, such as employees of the assessment office, assessment software administrators and security officers (CISOs).

## 1.2. Scope: digital and paper assessment

This workbook covers the entire assessment cycle (see figure 1 on page 10) and also looks at non-digital process stages that are required in order to take paper-based tests. We focus in particular on the forms of assessment where the questions need to be kept secret prior to the assessment taking place. This generally applies to all high-stakes[1] assessments, whether on paper, digital or oral. For types of assessment such as assignments, the tasks are not kept secret beforehand. When processing the results of this type of test, an institution should seek to follow the stages of the process: after all, nobody actually wants grades to be illegitimately tampered with or for archived tests to become lost.

In addition, we look at the CIA Triad aspects of Integrity and Confidentiality – see table 1 for an explanation of the terms used.

- *Availability:* this is primarily a technical area, which is highly important for digital assessment and in particular while the assessment is underway. Availability is also influenced by the choice between self-hosting or a cloud solution for the assessment software.
- *Bring Your Own Device (BYOD) in relation to digital assessment:* a number of institutions are successfully exploring this, but there is still insufficient knowledge and experience in this domain to include it in this first edition of the workbook.

[1] High-stakes assessments are tests where a lot is at stake for the student, e.g. an assessment that establishes the final grade for a subject.

| Term | Meaning |
|---|---|
| CIA Triad | A CIA Triad or CIA code is a code that rates the confidentiality (exclusivity), integrity (reliability) and availability (continuity) of the information and systems.[2] This classification is commonly used in the context of information security. |
| Confidentiality | A quality feature of the data. Confidentiality means that a piece of data can only be accessed by someone who is authorised to do so. |
| Integrity | Ensuring that the information matches the facts: information is correct, complete and up to date. |
| Availability | Indicates how often an IT service, system or component is accessible to authorised users. Availability is generally represented as a percentage. |

Table 1. Terms used

### 1.3. Responsibility

When compiling this workbook, we used the Conceptual framework for digital assessment[3] and the Secure Digital Testing guidelines[4]. The guidelines go into detail about the digital assessment administration process. This workbook focuses on securing the entire assessment chain and is not restricted to the test administration. Both publications can be used in parallel.

The starting point for this workbook is an analysis of the assessment processes in five institutions. Based on this, and working with the assessment experts from these institutions, a "model" assessment process is described (Appendix 1). The model assessment process is then used to map out in detail the risks at each stage of the assessment cycle and to formulate mitigation measures. This proposal was reviewed by the above assessment experts and a number of security officers in higher education. See the Acknowledgements page for an overview of all those involved in the creation of this workbook.

[2] https://nl.wikipedia.org/wiki/BIV-classificatie
[3] Digital test terminology (SURF, 2013) https://www.surf.nl/en/knowledge-base/2013/digital-test-terminology.html
[4] Guidelines for Secure Digital Assessment [Richtsnoer Veilige digitale toetsafname] (SURF, 2014; in Dutch only) https://www.surf.nl/kennisbank/2013/richtsnoer-veilige-digitale-toetsafname.html

INTERMEZZO

# EXAMPLES OF ASSESSMENTS IN PRACTICE: RISKS AND POINTS TO LOOK OUT FOR

In describing a number of practical situations, we show where the risks and points to look out for are in the assessment process. The examples are intended solely for illustration purposes. Other risks may also be present in reality. Each situation is described in the first instance for institutions that do not have this type of assessment security in place, and subsequently from the point of view of institutions that do have it.

## JOINTLY PREPARING AND REVIEWING ASSESSMENT QUESTIONS

Two lecturers at a higher educational institution are jointly preparing assessment questions for their subject.

**Unsafe practice**

Both lecturers regularly work on the assessment questions on their private tablet on the train using the on-board Wi-Fi. One lecturer originally created a Word document. They then send this document back and forth via email. They gradually flesh out the document and give it a version number to avoid confusion. One of them stores the document in Dropbox and the other one uses Google Drive. They ask a colleague to review the questions, who is almost always working at the same workstation. This colleague never locks her screen, nor does she lock up her office when she leaves briefly, e.g. to fetch a coffee.

**Safe practice**

Both lecturers work in different locations. When the two lecturers need to collaborate, they use a safe assessment environment set up specially by the institution. They save their shared document here. A colleague (an assessment expert) reviews the assessment questions for them. This colleague almost always works at the same workstation. The reviewing colleague and lecturer does not have access to the secure folder used by the first two lecturers and asks for a review version by email. They send him the encrypted Word document by email, but the password for the document by text message. In order to avoid any unauthorised persons gaining unapproved access to workstations, the screens at their workplaces always lock automatically after 10 minutes. In addition, lecturers are instructed to always lock their screens if they leave their workplace. The management makes sure that this is the case.

## PREPARING ASSESSMENTS

The lecturers have finalised 80 assessment questions. They will set an examination with 40 questions. A paper version of the exam also needs to be available for a number of special cases.

**Unsafe practice**

For a paper-based test they have agreed that one of them will pick 40 questions and copy them onto an USB stick. They place the USB stick in their mail pigeonhole in the lecturer's common room. The other lecturer picks up the stick from there and formats the questions according to the exam template. He uses his private tablet to do this because it is easier for him. He sends the test by email to an external print shop, because the in-house printer is busy all week.

**Safe practice**

For a paper-based test they have agreed that one of them will pick 40 questions and save them in the secure environment. The other lecturer formats them according to the correct exam template and organises the printing with the print shop because he is not authorised to print it himself from the exam environment. The print shop ultimately prints the exam papers that were delivered via the secure test environment. The lecturers deliver their examination through the secure environment, accompanied by a form containing numbers and other information. In the meantime, the assessment office is aware that the exam paper is arriving.

## PAPER TEST FORMS AT THE PRINT SHOP

The print shop prints the requested test forms.

**Unsafe practice**

The print shop prints the test forms and informs the back office that the exams are ready and can be collected. An employee from the back office is handed the forms in a sealed envelope, which he passes on to the lecturer who will be invigilating the exam. Because the exam will only take place one week later, the envelope spends a week lying on the lecturer's desk.

**Safe practice**

The print shop prints the paper versions of the exam no earlier than three days before the examination. Directly after printing, the forms are stored in a sealed envelope in the lockable storage area with a security camera, next to the print shop. The institution's rules say that the print shop has to deliver the forms to the assessment office 'just in time'. The assessment office ensures they are kept safe in a locked room with a strict access policy. The exam forms can only be collected one hour before the assessment by the lecturer or invigilator.

## SCORING TEST FORMS

The exam is over. One day after the examination, the results of the tests taken digitally are ready in the assessment application. The lecturers have collected the paper-based examination scripts from the back office. One lecturer performs the initial correction. A second lecturer checks the exams that have a grade of around 6 (out of 10).

**Unsafe practice**

The paper examination scripts spend the rest of the day sitting on the lecturer's desk while he is taking a class. There are six doubtful cases that the second scorer is taking a look at. He writes his own opinion on the paper exam scripts and overwrites the grade awarded earlier in the results list in Excel. The lecturer sends this file via email to the administration.

**Safe practice**

The lecturer is teaching for the rest of the day, and puts the examination scripts in his safe until he has time to look at them.

To log in to the safe environment, an extra access code is needed. The lecturer elects to receive this code via text message. There are six doubtful cases that the second scorer looks at. He writes his own assessment on the examination scripts. A typing error in the digital results list is easy to make (it is in the safe environment). The lecturer therefore leaves the original grade from the first scorer in both the paper version and the digital summary list. He adds his own grade in a separate column so that the history is clearly visible.

## REVIEWING EXAMINATION SCRIPTS – STUDENTS

At a certain point, students can review their own script (either digitally or on paper) in the examination area.

**Unsafe practice**

The students see their results in the grade centre in the digital environment, but the lecturer has forgotten to pass them on to the assessment office; the employees in the office make sure that students have read-access only and cannot access other applications. Now they have both read- and write-access and can access other Internet applications. The lecturer trusts his students not to publish the examination questions by email to the rest of the world immediately. Those who took their examination on paper can review them in the lecturer's office. The lecturer does not believe that the students will sneak in and change their answers. It simply will not happen. He sometimes has six students or more in his room at the same time.

If a student does not agree with his grade, he discusses it with the lecturer. The lecturer can change the grade and also update it immediately in the system.

**Safe practice**

At a certain point, students can review the assessments they conducted digitally in a grade centre within the secure assessment environment to which they have no access e.g. email. They only have read-access. If they have questions, they can ask them on the spot to the lecturer who is present. Those who conducted their assessment on paper can review these in the lecturer's office. They are called in two at a time. The lecturer remains in the room with them. Mobile phones are not allowed, and the students' bags are placed next to the lecturer. In this way, the lecturer makes sure that the students have no access and are unable to gain access to anything except what they are given. His desk is always empty. And he is not allowed to keep paper examination scripts in his own locker.

If a student does not agree with his grade, he discusses it with the lecturer who is present. The lecturer makes a note of this and at the end of the day enters any corrections in the secure environment, where he always has to log in using double authentication.

## MANAGING ASSESSMENT

Once all the grades are final, the assessments and the assessment results for both the digital and the paper versions are archived.

**Unsafe practice**

The lecturer scores the digital tests and the results as "completed" in the test application.

The lecturer takes the pile of paper test forms back to his office. He places them in the cupboard with the other paper-based assessments. He has to keep the assessments for two years. Because he is chronically short of cupboard space, he throws a pile of "older" test forms in his rubbish bin. He has lost the key to the cupboard.

**Safe practice**

The lecturer scores the digital assessments and the results as "completed" in the secure environment. In order to log in, he needs an additional access code that he receives via text message.

The lecturer takes the pile of paper test forms to the safe room that the institution has installed for this purpose. He signs the access list before entering, so that there is always traceability of who has been inside. A limited number of employees within the institution have access to this room.

# 2 SECURITY RISKS IN THE ASSESSMENT PROCESS

This chapter describes where to identify risks within the assessment process. It offers you starting points for carrying out a risk analysis at your own institution, and for correctly implementing the resulting measures. In this chapter you will also find an overview of factors that can help to make creating a secure assessment procedure successful.

The assessment cycle (see figure 1) is the starting point for the risk analysis. Based on the experiences of the five institutions, we have presented the risk analysis based on the seven stages in the assessment cycle, shown in table 2.


**Figure 1.** Assessment cycle (from the conceptual framework for digital assessment)

### 2.1. Risk analysis

In table 2 we show an overview of the most significant security risks for each sub-process of the assessment cycle, of the probability that they will occur and of their impact on both integrity and confidentiality. This analysis was created in collaboration with experts from the institutions. Our advice is to use this analysis as your starting point, to check it against the practices in your own institution, and ignore items or add to them where necessary.

The rating of high/medium/low is based on practical experience and may vary per situation. The table shows where the major risks exist in assessment, i.e. while administering a test. In practice, many measures are applied at this time to mitigate risks. At the same time, the table shows that there are also some fairly major risks during other stages of the process too. This workbook therefore provides an overview of measures to mitigate security risks at all stages of the process.

| STAGE OF PROCESS | PROBABILITY | IMPACT | | HIGHLIGHTS FOR EACH STAGE IN THE PROCESS |
|---|---|---|---|---|
| | | I | C | |
| Planning | L | L | L | The *planning* stage of the process does not involve any critical elements for security. The assessment matrix is not secret. The risk of security being threatened is therefore small. Process management focuses mainly on the quality of the content. |
| Construction | M | H | H | Lecturers *construct* assessment questions. They usually do so on their PC (laptop, tablet), after which they store drafts 'somewhere' (hard drive, Dropbox, USB stick, etc.) and email them to colleagues for review. None of this is very secure at all unless measures are taken. If examination material is leaked ahead of time, the damage can be significant. |
| Test administration | H | H | H | While the *examination is underway*, many things can go wrong: cheating, unauthorised tampering with digital assessments, losing or deleting results, etc. |
| Scoring | M | H | H | During the *scoring process* it is conceivable that there could be (digital) tampering with the results, or that assessments could go missing or otherwise become corrupted. |
| Analysis | L | H | M | During *analysis*, the risk primarily comes from tampering with results and the pass mark (standardised set). |
| Reporting | M | H | H | *Reviewing*, especially on paper, is a step that is especially susceptible to fraud. This includes things like tampering with the replies or unauthorised copying of assessment questions. In addition, the reported results are confidential. |
| Evaluation | L | M | M | *Evaluations* involve all of the exam programs, assessment materials and assessment results. Although integrity (exam programs) and confidentiality (materials and results) are important aspects, they are always implemented after a delay and are not traceable to an individual. Given that between evaluation and reuse there is a period of revision and potentially recovery available, there is no major risk during the evaluation part of the process. |
| Managing | M | H | H | If unauthorised tampering occurs during the *storage* of assessment questions, examination scripts and/or assessment results, or if materials get lost, this affects the demonstrability and/or legitimacy of the assessment. |

**Table 2** Security aspects per sub-process of the assessment cycle.
I=integrity; C=Confidentiality; L=low; M=medium; H=High.

In this workbook we are making the following assumptions:

a. If the risk is *Low*, there is no (or no urgent) need to apply additional measures.
b. Where the risk is *Medium*, it can be assumed that it is adequately covered provided that the *Baseline for information security in Higher Education* (see frame on page 12) has been implemented correctly.
c. If the risk is *High*, then additional measures are needed.

The higher education institutions in the SURF Community for Information Security and Privacy (SCIPR) have jointly defined a baseline in the area of information security. If institutions comply with this, it means that the information security around and within higher education meets an acceptable baseline. The full implementation of this baseline within the institution delivers generic information security at a medium level. The baseline is based on ISO 27002:2013, an internationally accepted set of standards.

The baseline covers virus protection, the use of passwords and the use of firewalls. The full baseline is itself an extensive document. We will not go into this area in detail in this workbook.

**Frame** Information about the Baseline for Information Security

### 2.2. Success factors for secure solutions

The institutions involved clearly state that securing the assessment chain is a complex process featuring a significant "human element" combined with a technical approach. We cover a number of factors that will make an important contribution to successfully establishing a secure assessment process:

- Uniformity in the assessment process improves its predictability and therefore makes it easier to manage; being easy to manage is a precondition for being able to remain in *control* and to anticipate potential incidents.
- *Keep it simple*. This is how to make working securely easy to explain and to keep it simple in practice. This is how you avoid people within an institution looking for alternatives or taking shortcuts.
- As far as possible, base things on what you are already doing in terms of security within the institution, and pay plenty of attention to ease of use. If a work instruction is too complicated, people will work around it.
- A safe organisation (people) and technology are both important.
- Security is something people have to do, which means that awareness is crucial. Talk about security regularly, so that you can pick up on attitudes and behaviour within the organisation.

# 3 TOWARDS A SECURE ASSESSMENT PROCESS

In this chapter you can see which steps you as an institution need to take to ensure a secure assessment process.

### 3.1. Overview of stages

Which steps does an institution need to take in order to have a secure assessment process? How is assessment security guaranteed throughout? This is shown in a highly simplified manner in figure 2. In the following section, we explain what each of the separate stages are.

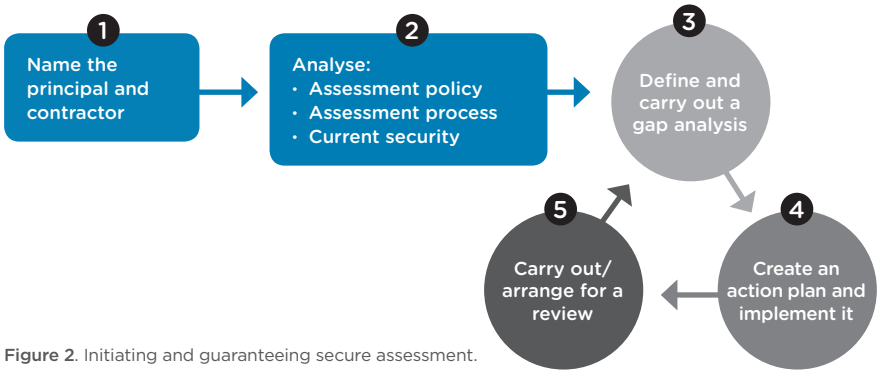



**Figure 2**. Initiating and guaranteeing secure assessment.

### 3.2. Stage 1: Task and ownership

It is important to distinguish between the initial activity required to secure the assessment process more effectively and how to maintain it. On this basis, securing the assessment process can be tackled procedurally or as a project. The latter is recommended if you expect that major work needs to be done to reach a high standard.

A difficult question that should always be asked and answered is: who is or will be the principal and therefore the owner of “secure assessment”? This is closely linked to the question of who has (or will have) a mandate to push this along the entire chain. This role can be taken by the Planning & Control manager, a Director of Education or – and this is a relatively new role that institutions are creating more frequently – the Chain Manager for Assessments.

A chain manager for assessments (also the “process owner for assessments”) is specifically responsible within the institution for the entire assessment process and has the authority to intervene wherever he/she deems it necessary. This role is ideally suited for a dean, as he/she can manage the issue from within the core process.

### 3.3. Stage 2: Analysis of current situation

The analysis of the current situation is focussed on three aspects: the assessment policy in relation to assessment security, the effect of the assessment process, and the information security policy at the institution.

**a.** Find out what the institution's assessment policy defines in terms of assessment security. In most cases, the assessment policy will at least address a number of aspects of fraud. The approach to assessment security needs to be aligned with these aspects.
**b.** Describe the assessment process of the institution; you may wish to use the detailed examples described in Appendix 1 of this workbook.
**c.** Find out what regular information security measures are in place within the institution; we recommend that you collaborate here with the information security officer for your institution. If the measures comply with the published baseline for information security in higher education, then you have at least a solid basis in place that will give you the "middle" level for assessments. This means that where a "high" security level is needed, additional measures will be necessary. You will find tools for this in Appendix 2.

### 3.4. Stage 3: Gap analysis

**d.** Once the current situation has been mapped out, you can carry out a gap analysis. As you need to look in detail at the security of the assessment process, this can prove to be a major job. In Appendix 3, we provide an extensive tool which you can use as a checklist. Here, too, you need to pay most attention to the risks that are rated 'high'. Evaluate and discuss the gaps you discover with the stakeholders and those affected.

### 3.5. Stage 4: Action plan for secure assessment

**e.** Create an action plan: jointly define the priorities and the approach to applying measures. For this, make use of the example measures in Appendix 3.
**f.** Carry out the action plan. Apply priorities if it turns out that there are many measures required. The measures need to be aimed at ensuring the actors involved work securely (awareness) and at technical aspects.

### 3.6. Stage 5: Review

**g.** Now perform a self-review or have an external review carried out of the improved security of the assessment process. Appendix 4 provides a point of comparison for this. This stage is important to validate the measures that were taken and thereby ensure the intended security of the assessment process was in fact delivered.

### 3.7. Future-proofing secure assessment

If assessment security is at the desired level, the next job is to ensure it remains like this. That requires:

- an owner of the secure assessment process, as well as the chain manager or process owner for testing as stated above.
- regular monitoring of the status of assessment security and, if necessary, implementation of additional measures, i.e. effectively repeating the individual stages from c to e above.
- regular attention to the awareness of all actors in the assessment chain.

# 4 CONCLUSION

Ensuring that the assessment process as a whole is structurally secure is not a simple task. In fact, we believe it is a necessary exercise given the importance of the legitimacy of assessments in higher education.

---

This workbook has been created thanks to the efforts of many different people. We are very grateful to all of them. At the same time, we realise that this is “only” version 1.0. Practice will show us what improvements, additions and corrections are necessary and possible. We therefore ask the users of this workbook to give us feedback. You can do this by sending an email to Annette Peet, project manager for Digital assessment at SURFnet, annette.peet@surfnet.nl.

# APPENDICES


## 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**

APPENDIX 1

# DETAILED EXAMPLE OF THE ASSESSMENT PROCESS

## Introduction

To achieve a secure assessment process, this workbook describes a number of stages in Chapter 3. The first stage involves mapping out the institution's assessment process in writing (*see also stage 2 in paragraph 3.3. on page 14*). This appendix offers a detailed description that can be used as an example to follow. You can use this as a guideline for developing your institution's assessment process or use it as a comparison to test against.

This detailed example was created from an analysis of the assessment process at the five institutions that collaborated in composing this workbook. This makes it the "common denominator" of the five institutions as an example, though the process may vary in any given institution. You can use this model to check for omissions.

It is important that the roles and responsibilities within the institution are clearly defined and managed. By the "assessment process", we mean all the stages of the assessment cycle plus assessment management (*see figure 1 on page 10)*. We describe the main process and the sub-processes based on the assessment cycle. Each sub-process is then broken down into activities and roles. The activities are classified and constitute the input for the risk matrix (*Appendix 3*).

The process assumes a digital approach; even when assessments are paper-based, digital preparation is frequently used, involving a word processing programme, email and digital storage.

## Structure of this Appendix

We provide a detailed description of each part of the process. This detail allows the process to be broken down into specific actions in order to make the assessment process more secure across each step. The format of the description for each part of the process is:

1. table of the main features of this sub-process;
2. process flow;
3. description of activities.

After the description of the sub-processes, we describe all of the roles. A RACI[5] table is also included.

[5] RACI is a widely-used methodology for classifying roles and responsibilities. The categories are Responsible, Accountable, Consulted and Informed.

## Structure of this Appendix


| | | |
|---|---|---|
| Key to symbols | | 18 |
| Process model for a secure assessment chain | | 19 |
| Sub-process 1: | Planning | 20 |
| Sub-process 2: | Construction | 22 |
| Sub-process 3a: | Test administration - digitally | 24 |
| Sub-process 3b: | Test administration - on paper | 26 |
| Sub-process 4: | Scoring | 28 |
| Sub-process 5: | Analysis | 30 |
| Sub-process 6: | Reporting | 32 |
| Sub-process 7: | Evaluation | 34 |
| Sub-process 8: | Managing | 36 |
| RACI for the entire assessment process | | 38 |


## Key to symbols

| | |
|---|---|
| ACTIVITY | An activity consists of a number of actions that a single 'actor' (a person, system or department) can carry out in a single consecutive period of time. |
| CHOICE OR DECISION POINT | While carrying out a process, there are always moments where choices need to be made or where circumstances or situations lead to multiple options that can be taken. |
| DOCUMENT OR FILE | Within a process, documents or files are created, moved, exchanged or amended. The symbol here can mean either documents or digital files. The designation is shown in the scheme and the process description in blue and italics. |
| COMMUNICATION | In contrast to the "solid" arrow ( ⟶ ) that shows flow, the broken line is used to show communication. Communication in the form of a discussion, information, etc., but can also mean sending an email, document or file. |
| OTHER PROCESS | This symbol indicates that there is an input or output flowing from/to another (sub-)process. |
| DATA STORAGE | Data storage, e.g. a hard disk |

# SECURE ASSESSMENT CHAIN
## PROCESS MODEL

**MAIN FEATURES**

**Process owner**
Course/programme manager

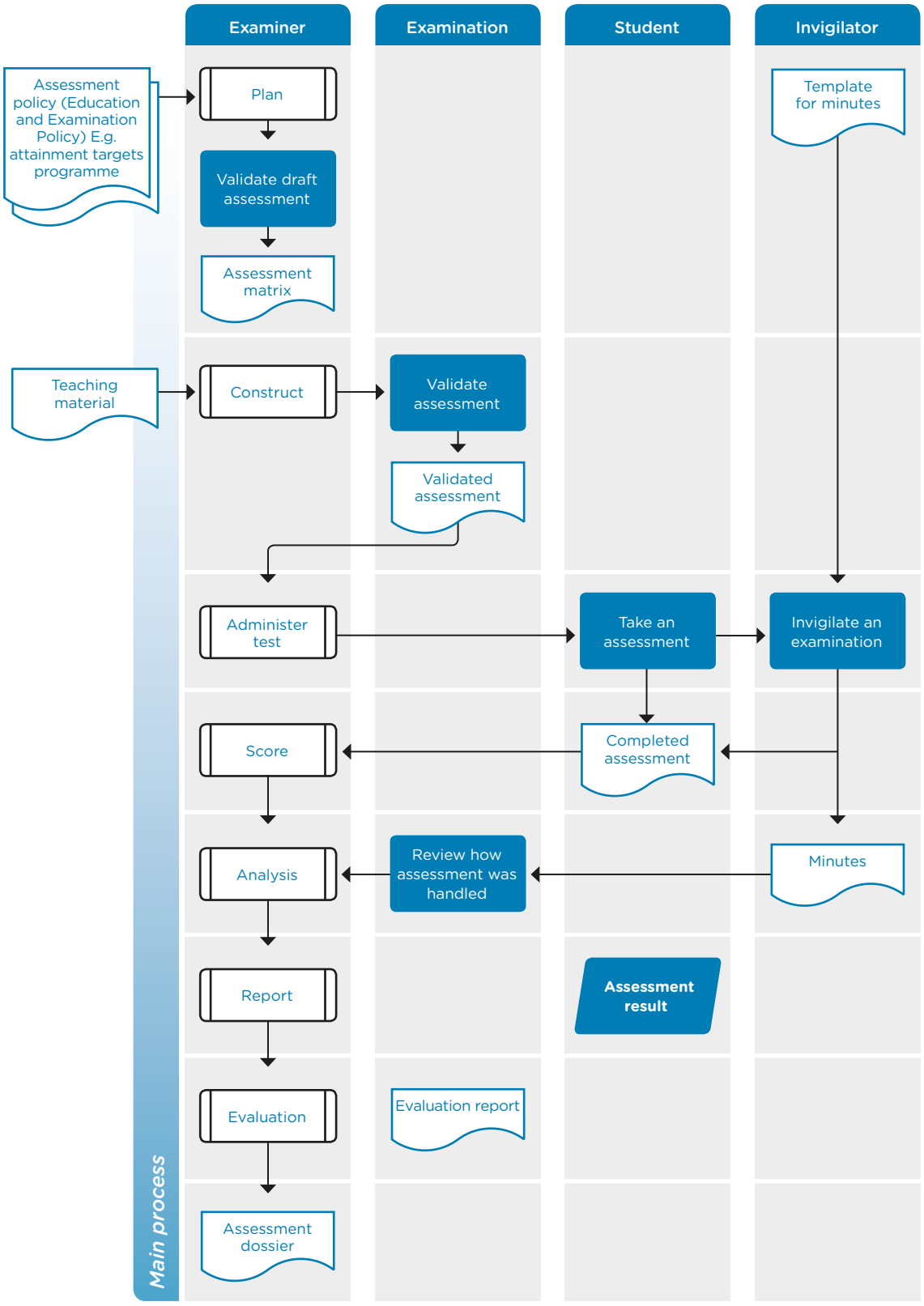
**Process description**
The entire process from planning to evaluation, including assessment management.

**Process goal**
Determining whether the student has the right knowledge and/or skills.

**Process precondition(s)**
The process is reliable (includes confidentiality, integrity, availability) and measurable.

**Input**
Unit for assessment based on examination programme.

**Output**
Study credits awarded correctly.



# SUB-PROCESS 1 PLAN

MAIN FEATURES

**Process owner**
Examiner

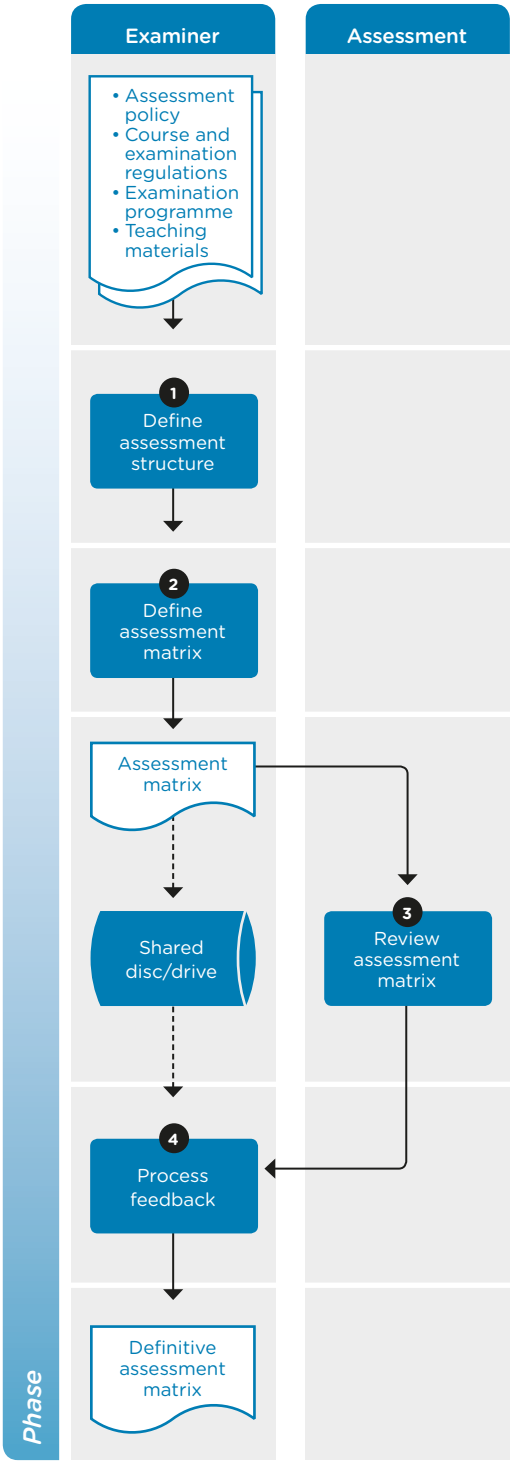
**Process description**
Students receive teaching materials to work on throughout the year. Doing it properly requires a well-thought-out approach

**Process goal**
The planning (specification) of an assessment.

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

**Input**
The current assessment policy, the Course and examination regulations, the assessment examination programme with the final criteria, the learning materials to be assessed and the opinions of the examiner about what is important and what must be assessed in which form.

**Output**
Finalised assessment matrix



## ACTIVITIES IN SUB-PROCESS 1: PLAN

| | Activity | How (procedural description) | When | Who |
|---|---|---|---|---|
| 1 | DEFINE ASSESSMENT APPROACH | The examiner defines the approach for the assessment. For this, he or she may consult various sources. | Throughout the year | Examiner |
| 2 | SET UP ASSESSMENT MATRIX | The examiner translates the assessment approach into an assessment specification (assessment matrix) and defines this in a document. He/she stores this document locally on a PC or on a network location and emails it to the assessment expert. It may also be stored in a learning management, assessment or generic collaboration system, to which peers and assessment experts have access. | | Examiner |
| 3 | REVIEW ASSESSMENT MATRIX | On request by the examiner, one or more experts review the assessment specification created by the examiner. They provide the examiner with educational feedback so that the examiner can define the best possible assessment matrix. | | Assessment expert |
| 4 | PROCESS FEEDBACK | The examiner processes the feedback from the reviewers and creates a definitive assessment specification. | | Examiner |

# SUB-PROCESS 2 CONSTRUCT

**MAIN FEATURES**

**Process owner**
Examiner

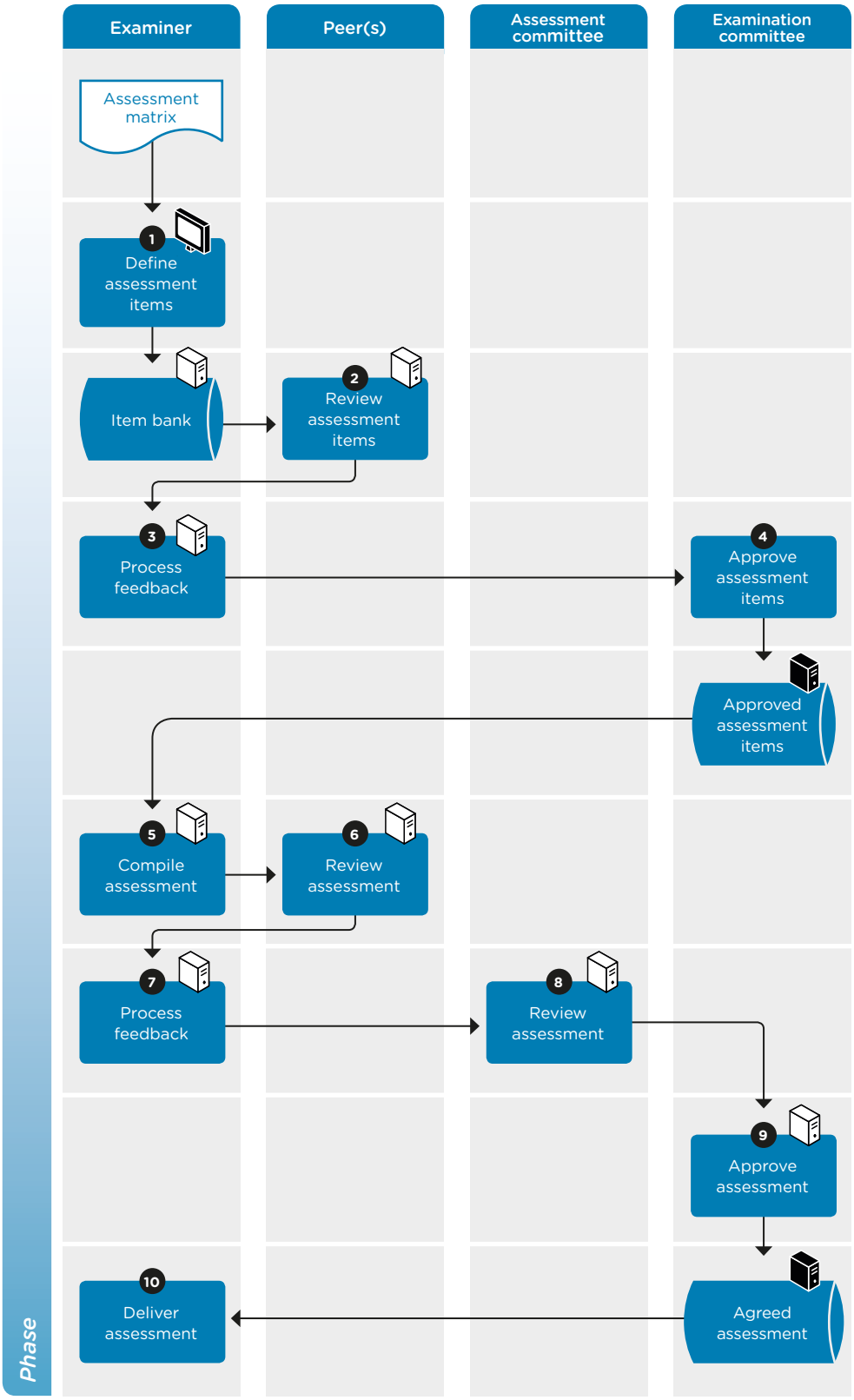
**Process description**
Proper testing requires the assessment to be formulated in a well-conceived manner. In the Construction sub-process the assessment is created.

**Process goal**
Good assessment/assessment items

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

**Input**
Assessment matrix, teaching material to be assessed.

**Output**
Agreed assessment items and assessment




Item bank

Item bank

Author environment

## ACTIVITIES IN SUB-PROCESS 2: CONSTRUCT

| | Activity | How (procedural description) | When | Who |
|---|---|---|---|---|
| 1 | DEFINE ASSESSMENT ITEMS | The examiner creates the assessment items on the basis of the assessment matrix. These are stored locally on a PC, tablet or on a network or cloud location, and passed on to an assessment expert. They may also be stored in a learning management, assessment or generic collaboration system, to which peers and assessment experts have access. Sometimes this may also involve documents on a USB stick. | Throughout the year | Examiner |
| 2 | REVIEW ASSESSMENT ITEMS | On request by the examiner, one or more colleagues review the assessment items drafted by the examiner. They provide the examiner with (educational) feedback so that the examiner can create the best possible assessment items. | | Peers |
| 3 | PROCESS FEEDBACK | The examiner processes the feedback from the reviewers and creates definitive assessment items. | | Examiner |
| 4 | APPROVE ASSESSMENT ITEMS | The examination committee defines the assessment items and approves them for use in assessments. | | Examination committee |
| 5 | COMPILE ASSESSMENT | The examiner compiles an assessment using the assessment matrix and the assessment items. This is stored locally on a PC, tablet or on a network or cloud location, and passed to an assessment expert. It may also be stored in a learning management, assessment or generic collaboration system, to which peers and assessment experts have access. On occasion, this may also involve the storing of documents on a USB stick. | Two weeks before the assessment | Examiner |
| 6 | REVIEW ASSESSMENT | On request by the examiner, one or more colleagues review the assessment drafted by the examiner. They provide the examiner with (educational) feedback so that the examiner can create the best possible assessment. | | Peers and the assessment committee as required |
| 7 | PROCESS FEEDBACK | The examiner processes the feedback from the reviewers and creates a definitive assessment. | | Examiner |
| 8 | REVIEW ASSESSMENT | The assessment committee reviews the assessments prepared by the examiner before they are approved. | | Assessment committee |
| 9 | APPROVE ASSESSMENT | The examiner processes the feedback to create the definitive assessment. | One week before the assessment | Examiner |
| 10 | DELIVER THE ASSESSMENT | The examiner delivers the digital or paper assessment before it is held. | (Immediately) before the examination/ assessment weeks | Examiner |

# SUB-PROCESS 3a

## TEST ADMINISTRATION – DIGITAL

**MAIN FEATURES**

**Process owner**
Examiner

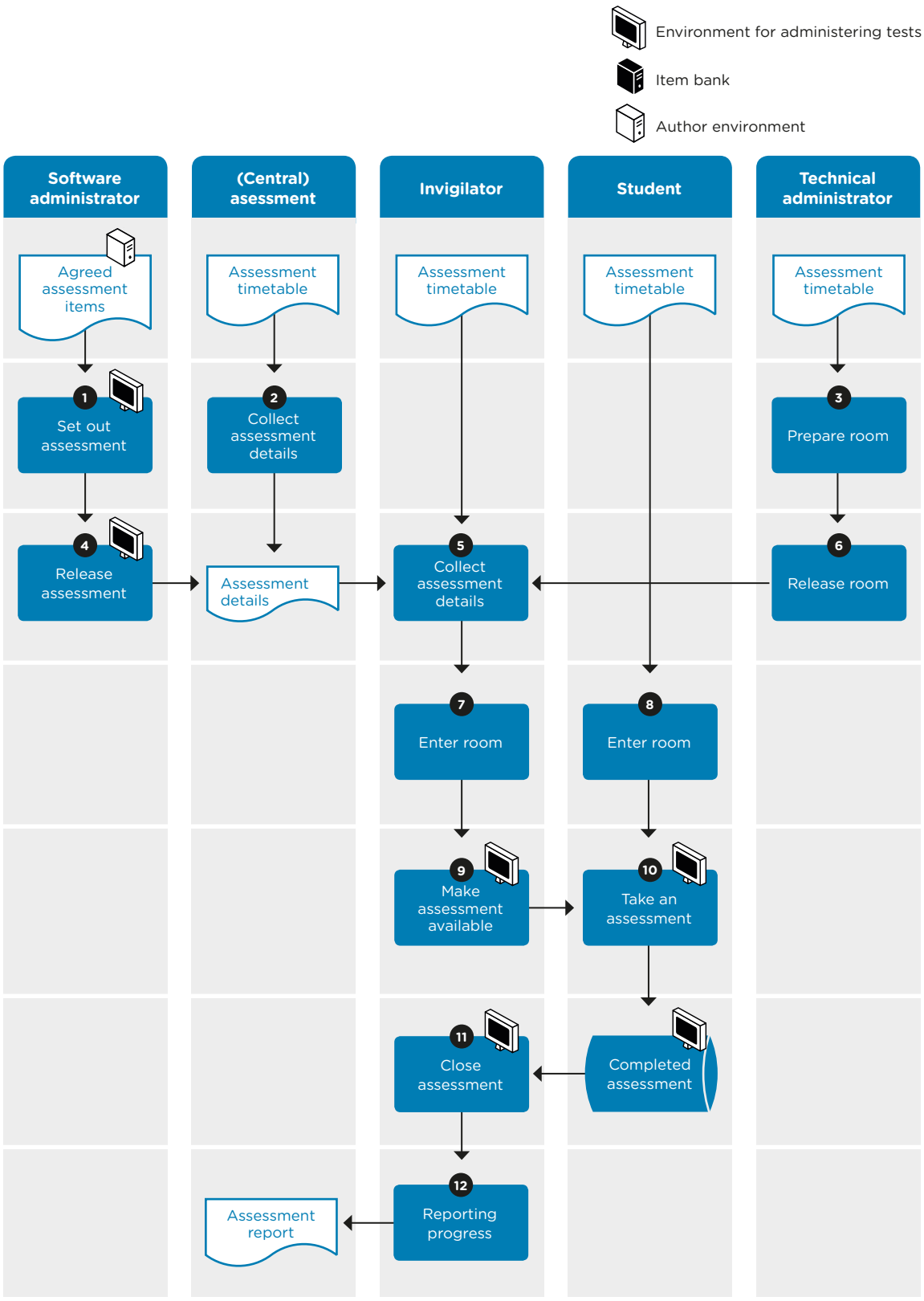
**Process discription**
Administering the test

**Process goal**
Assess students in a reliable and auditable way.

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

**Input**
Agreed assessment items, assessment timetable

**Output**
Completed assessments, assessment report (log)



## ACTIVITIES IN SUB-PROCESS 3a: ADMINISTRATION - DIGITAL

| | Activity | How (procedural description) | When | Who |
|---|---|---|---|---|
| 1 | MAKE ASSESSMENT READY | The complete assessment is sent to the software administrator, who prepares it in the examination environment of the assessment system. | Until the day before the assessment | Software administrator |
| 2 | COLLECT ASSESSMENT DETAILS | The assessment coordinator collects all the information relating to the assessment. | Until one hour before the assessment | Assessment coordinator |
| 3 | PREPARE ROOM | The room is prepared for the assessment. These preparations may include activities such as setting up tables correctly, installing partitions, preparing examination PCs and providing equipment to disabled students. | Until one hour before the assessment | Room manager |
| 4 | RELEASE ASSESSMENT | Prior to the actual moment of the assessment, the assessment is released in the assessment system. If there are candidates who are administering the tests on paper, e.g. due to disabilities, the assessment coordinator prints out the assessment items on paper and keeps them until the invigilator comes to collect the assessment details. | Until one hour before the assessment | Software administrator |
| 5 | COLLECT ASSESSMENT DETAILS | From the assessment coordinator, the invigilator collects everything that is needed for the examination session to run smoothly. The assessment details include at least the following:<br>• Contact details of management;<br>• List of candidates;<br>• Details of this examination session (start and end time, special provisions, open/closed book, etc.);<br>• Possible exceptions to the assessment regulations;<br>• Login codes for the system for taking the assessment;<br>• Template for assessment report and log;<br>• Printed assessments (as required). | One hour before the assessment | Invigilator |
| 6 | OPEN ROOM | Once the room is ready for the assessment session, the key to the room is available for the invigilator to collect. | One hour before the assessment | Technical administrator |
| 7 | ENTER ROOM | The invigilator opens the room and checks that the room is in the condition stated in the assessment details. | Half an hour before the assessment | Invigilator |
| 8 | ENTER ROOM | Just before the start of the assessment (as shown in the assessment details), the students included on the candidate list are allowed into the room. | Fifteen minutes before the assessment | Student |
| 9 | MAKE ASSESSMENT AVAILABLE | At the time stated in the assessment details, the invigilator makes the assessment available for candidates to log in or hands out the paper assessments. | Five minutes before the start of the assessment | Invigilator |
| 10 | PERFORM ASSESSMENT | The candidates take the assessment. Candidates who are finished log out of the examination system or hand in the completed assessment to the invigilator. Leaving the assessment room temporarily is permitted if it is set out in the assessment details; any preconditions are also in the assessment details. | | Student |
| 11 | CLOSE ASSESSMENT | If not pre-set in advance, the invigilator closes the assessment in the assessment system at the end of the assessment period. Once closed, it is no longer possible to make changes in the the examination environment. | At the end of the assessment period | Invigilator |
| 12 | REPORT PROGRESS | After the end of the assessment, the invigilator completes the log. The log has a fixed template which allows the progress of the assessment to be recorded systematically together with any exceptional items. Urgent exceptional items during the course of the assessment are agreed by phone between the invigilator and the assessment coordinator and/or managers. | Within one hour after the end of the assessment | Invigilator |

# SUB-PROCESS 3b

## TEST ADMISTRATION – ON PAPER

MAIN FEATURES

**Process owner**
Examiner

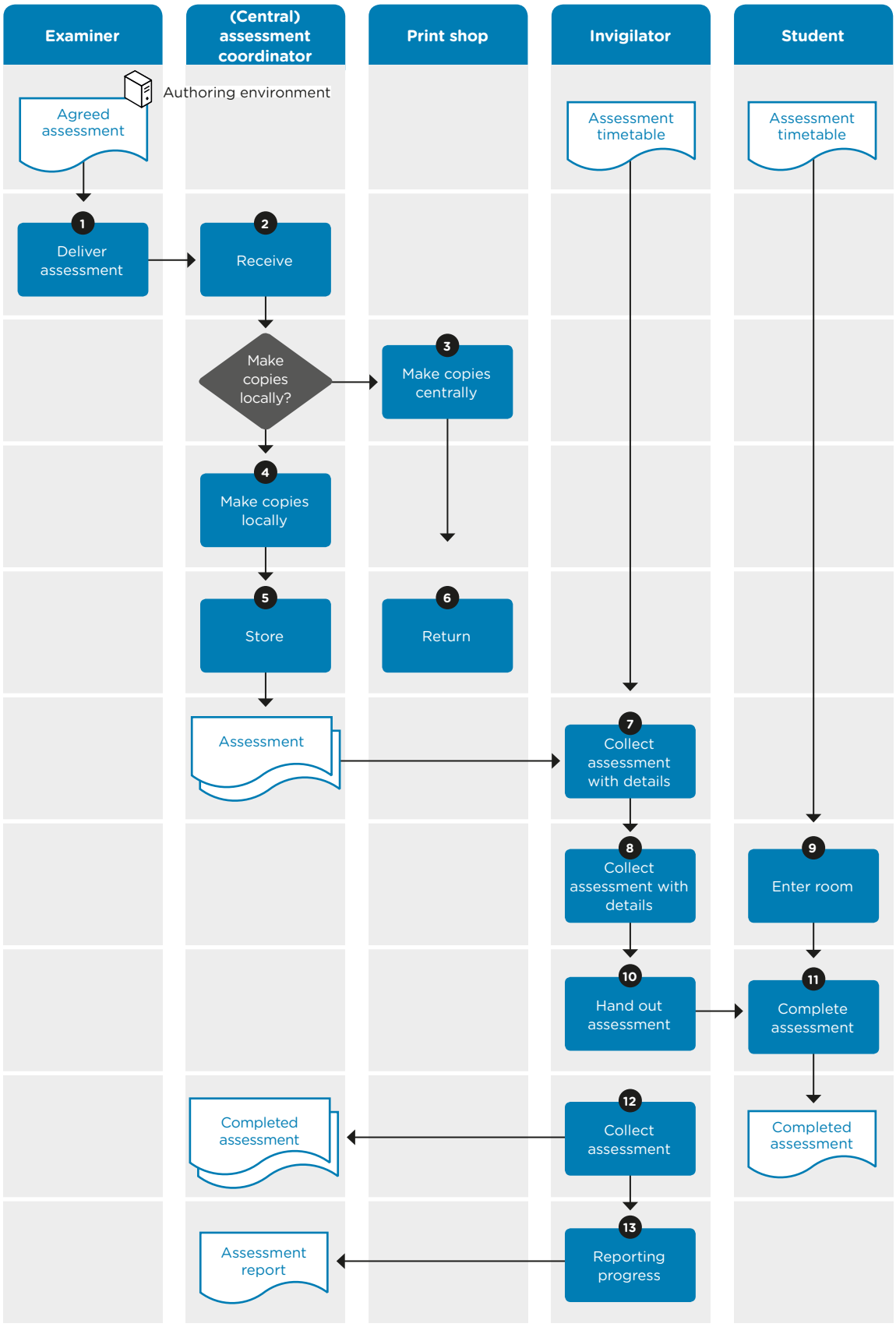
**Process description**
Administering the test

**Process goal**
Assess students in a reliable and controlled way.

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

**Input**
Agreed assessment items, assessment timetable

**Output**
Completed assessments, assessment report (log)



## ACTIVITIES IN SUB-PROCESS 3b: TEST ADMINISTRATION - ON PAPER

| | Activity | How (procedural description) | When | Who |
|---|---|---|---|---|
| 1 | DELIVER THE ASSESSMENT | The examiner delivers the prepared assessment to prepare for the examination session. Generally speaking, delivery is made digitally. | Until one week before the assessment | Examiner |
| 2 | RECEIVE | The assessment coordinator receives the original of the assessment and keeps it until it is to be copied. | Until one week before the assessment | Assessment coordinator |
| 3 | COPYING CENTRALLY | The original of the assessment is sent to the print shop. | One day before the assessment | Assessment coordinator |
| 4 | COPYING LOCALLY | The assessment coordinator personally makes sure the number of copies required of the original assessment are produced. | One day before the assessment | Assessment coordinator |
| 5 | STORAGE | The copied assessment is stored until it is needed in the examination room. | | Assessment coordinator |
| 6 | OPEN ROOM | The key to the room is made available to the invigilator at the agreed time before the assessment. | One hour before the assessment | Technical administrator |
| 7 | COLLECT ASSESSMENT DETAILS | From the assessment coordinator, the invigilator collects everything that is needed for the examination session to run smoothly. The assessment details include at least the following:<br>• Contact details of management;<br>• List of candidates;<br>• Details of this examination session (start and end time, special provisions, open/closed book, etc.);<br>• Possible exceptions to the assessment regulations;<br>• Template for assessment report and log;<br>• Printed assessments. | One hour before the assessment | Invigilator |
| 8 | ENTER ROOM | The invigilator opens the room and checks that the room is in the condition stated in the assessment details. | Half an hour before the assessment | Invigilator |
| 8 | ENTER ROOM | Just before the start of the assessment as specified in the assessment details, the students included on the candidate list are allowed into the room (by the invigilator). | Half an hour before the assessment | Student |
| 9 | HANDING OUT ASSESSMENT | At the time stated in the assessment details, the assessment is handed out to the students who meet the admission criteria. | Fifteen minutes before the assessment | Invigilator |
| 11 | PERFORM ASSESSMENT | The candidates take the assessment. The candidates who are finished hand in the completed assessment to the invigilator. Leaving the assessment room temporarily is permitted if it is allowed in the assessment details. Any preconditions are also included in the assessment details. | | Student |
| 11 | COLLECT ASSESSMENTS | At the end of the examination period, the invigilator asks students to stop working on the assessment and to hand in the assessments. | | Invigilator |
| 12 | REPORT PROGRESS | After the end of the assessment, the invigilator completes the log. The log has a fixed template which allows the progress of the assessment to be recorded systematically together with any exceptional items. Urgent exceptional items during the course of the assessment are agreed by phone between the invigilator and the assessment coordinator and/or managers. | Within one hour after the end of the assessment | Invigilator |

# SUB-RPOCESS 4 SCORING

**MAIN FEATURES**

**Process owner**
Examiner

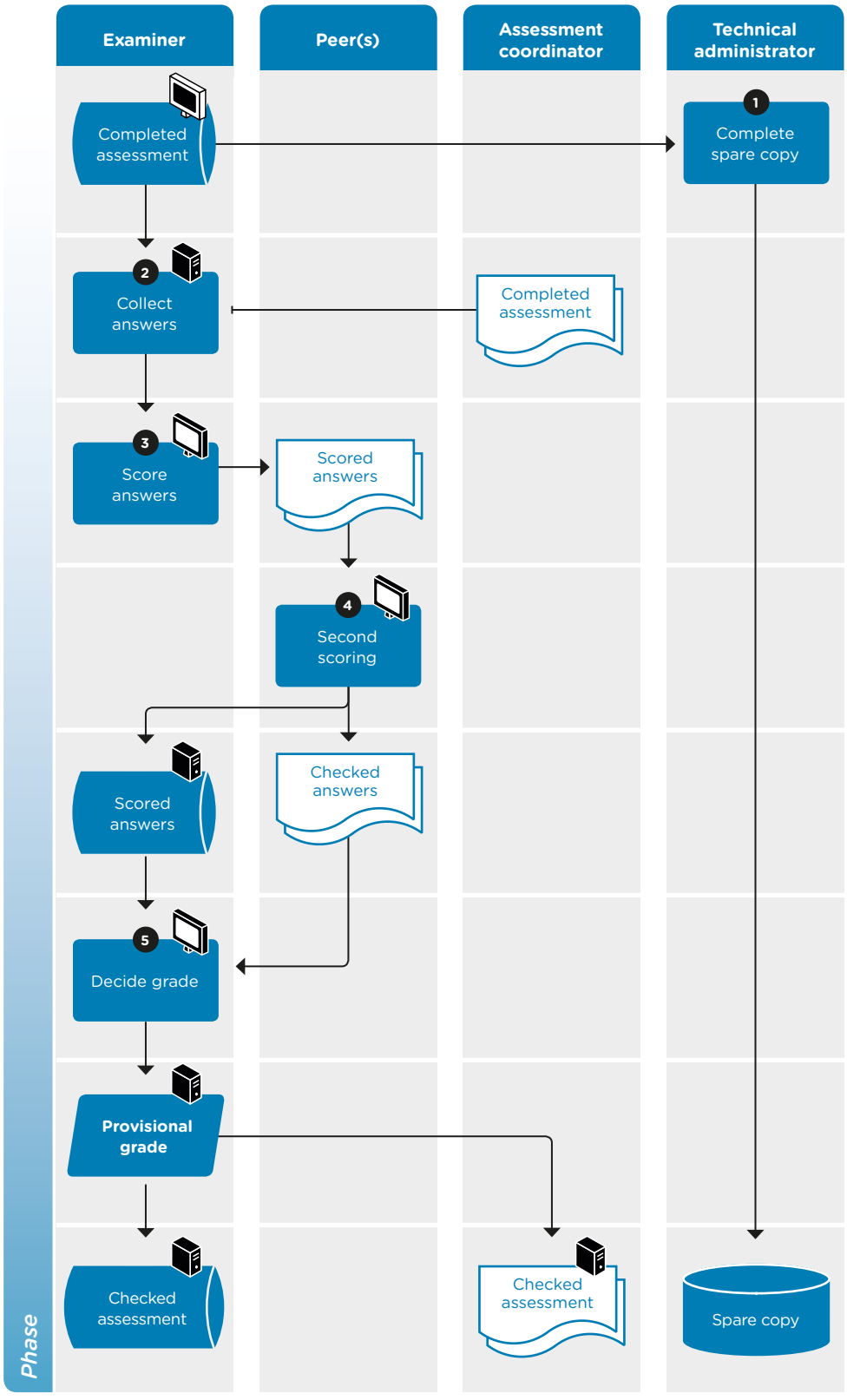
**Process description**
Scoring the completed questions and assigning a provisional grade to answers, in line with the standard.

**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




Item bank

Item bank

Delivery environment

## 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 |

# SUB-PROCESS 5 ANALYSE

MAIN FEATURES

**Process owner**
Examiner

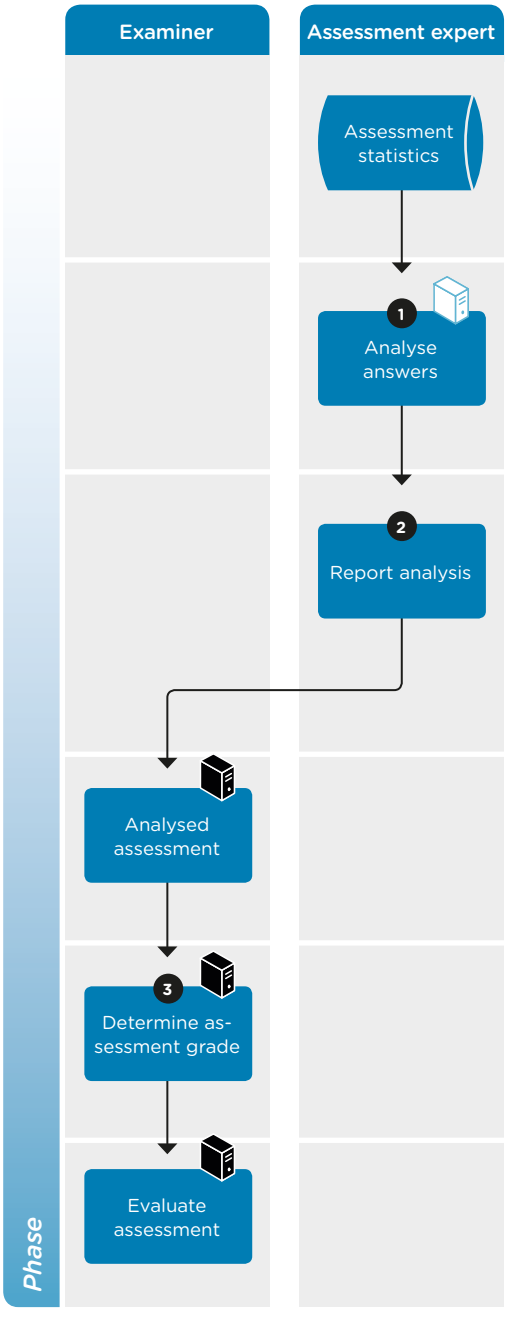
**Process description**
Identifying items that were of poor quality, for example because they appear to be too easy, too difficult or ambiguous. These items are set aside when determining the grade.

**Process goal**
Correction of the standard to increase the reliability of the assessment and the value of the answers.

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

**Input**
Replies to the assessment questions, standardisation

**Output**
Checked questions and standardisation




Item bank

Analysis environment

## ACTIVITIES IN SUB-PROCESS 5: ANALYSE

| | Activity | How (procedural description) | When | Who |
|---|---|---|---|---|
| 1 | ANALYSE ANSWERS | The assessment expert checks the reliability of the assessment based on statistics in the item bank and/or (e.g.) Excel spreadsheets from the assessment package. | After scoring | Assessment expert |
| 2 | REPORT ANALYSIS | The assessment expert reports his/her findings to the examiner. He/she may advise the removal of certain questions and/or revision of the pass mark. | Within SMART agreement | Assessment expert |
| 3 | DETERMINE GRADE | The examiner finalises the grade based on the checked assessments (paper or digital) and the definitive agreed pass mark. | Within the period required by the Course and examination regulations | Examiner |

# SUB-PROCESS 6 REPORT

**MAIN FEATURES**

**Process owner**
Examiner

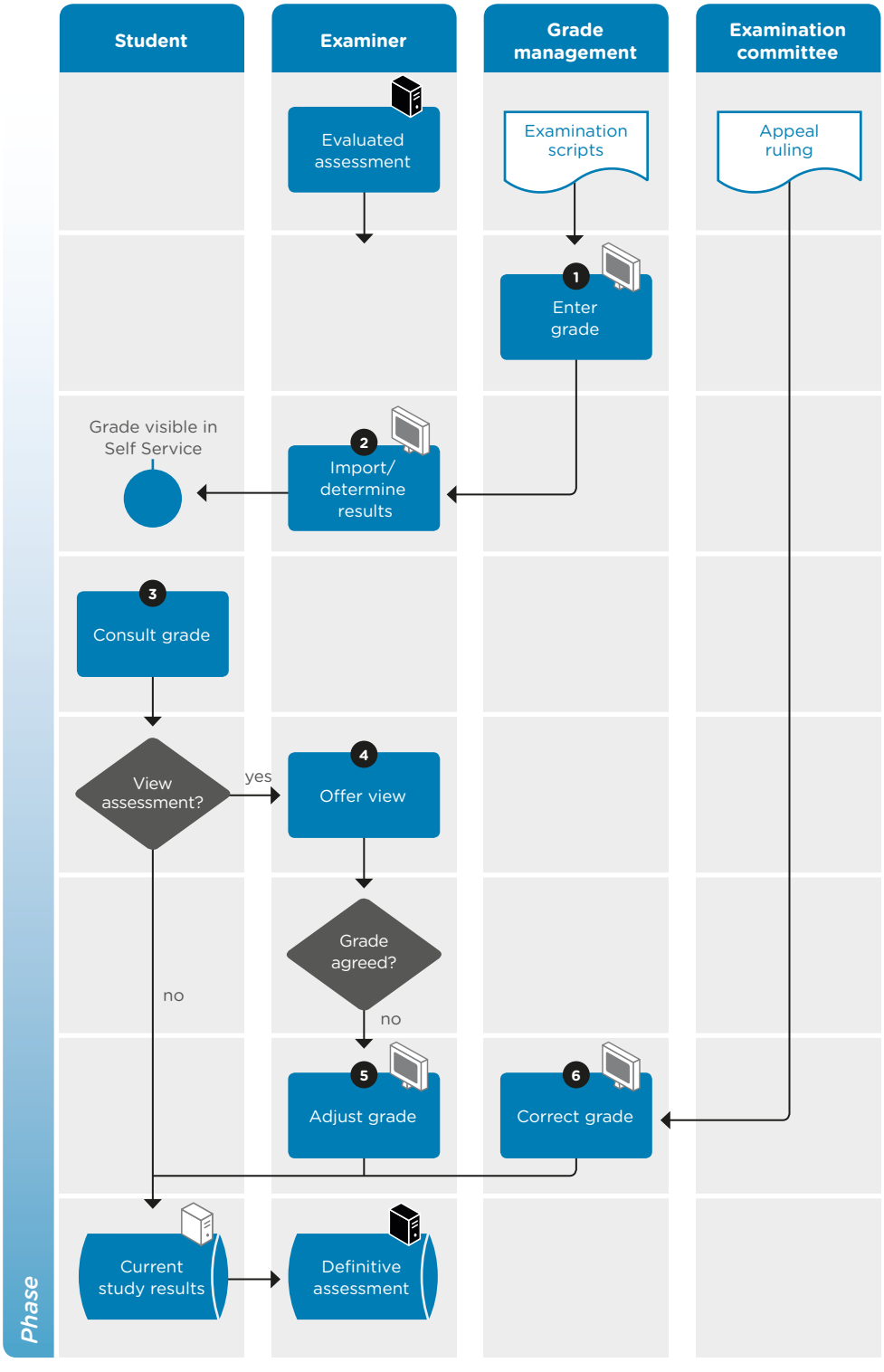
**Process description**
Link back to the assessment results

**Process goal**
Inform students in a reliable and controlled manner of their results and offer option to view details.

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

**Input**
Evaluated assessment

**Output**
Communicated result




SIS

Item bank

SIS

## ACTIVITIES IN SUB-PROCESS 6: REPORT

| | Activity | How (procedural description) | When | Who |
|---|---|---|---|---|
| 1 | ENTER GRADES | Examination results slips may be used (whether digital or not). The examiner delivers these to the grade administration. The grade administration then defines the results in the electronic learning environment and/or SIS. | Within 1 day of receipt | Grade administration |
| 2 | IMPORT/ DETERMINE RESULTS | The examiner is responsible for the grades. He/she releases the results to the students. This can be done in three ways:<br>• grades delivered via a link to the assessment system as draft in the SIS, the examiner checks and releases;<br>• administration has entered the grades; examiner just needs to re-check and release;<br>• examiner enters the grades himself and releases. | Within 1 day of entry | Examiner |
| 3 | VIEW GRADE | As soon as they are released by the examiner, the student can view the grades in the electronic learning environment and/or SIS. | Within the period required by the Course and examination regulations | Student |
| 4 | GIVE ACCESS | Assessments are available for reviewing. When reviewing, those who conducted the assessment can discuss the replies and the norming of the completed task. | Within the period required by the Course and examination regulations | Examiner |
| 5 | ADJUST GRADE | The examiner has the ability to change grades during a period following the administering of the test as defined in the Education and Examination Policy. | Within the period required by the Course and examination regulations | Examiner |
| 6 | CORRECT GRADE | When required by an appeal decision, the grade administration can change the current result. | | Grade administration |

# SUB-PROCESS 7 EVALUATE

MAIN FEATURES

**Process owner**
Examiner

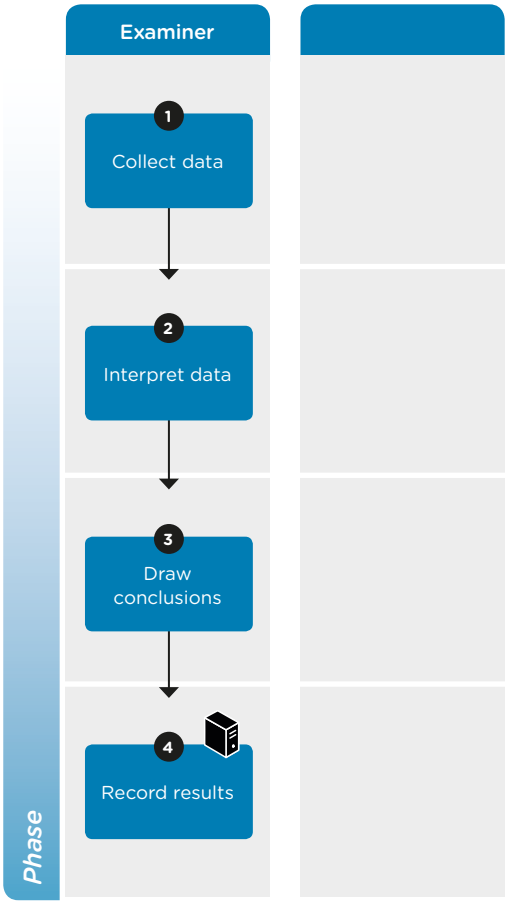
**Process description**
Used assessments (answers to completed assessments) are a valuable source for determining the quality of an assessment in practice. In sub-process evaluation, the quality of the various items and the assessment as a whole are evaluated on the basis of past/completed assessments, with the aim of achieving better evaluations, assessment items and/or assessment matrices.

**Process goal**
Constructing assessments that most closely match the purpose of the assessment.

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

**Input**
Assessment matrix, completed assessments, possible feedback from students.

**Output**
Improved assessment matrix and/or assessment (items); improved item bank.




Item bank

## ACTIVITIES IN SUB-PROCESS 7: EVALUATE

| | Activity | How (procedural description) | When | Who |
|---|---|---|---|---|
| 1 | COLLECT DATA | All information that is necessary, or expected to be necessary, is collected. | After completion of a few or a series of assessments | Examiner |
| 2 | INTERPRET INFORMATION | Bearing in mind the purpose of the assessments, review whether the validity and reliability (and possibly also the equity and usability) of the assessment is reasonable. | | Examiner |
| 3 | DRAW CONCLUSIONS | Making decisions about the quality of the reviewed assessments. | | Examiner |
| 4 | RECORD RESULTS | Determine the results so that peers can learn from this, and/or the item bank improves in quality. | | Examiner |

# SUB-PROCESS 8 MANAGE

MAIN FEATURES

**Process owner**
Examiner

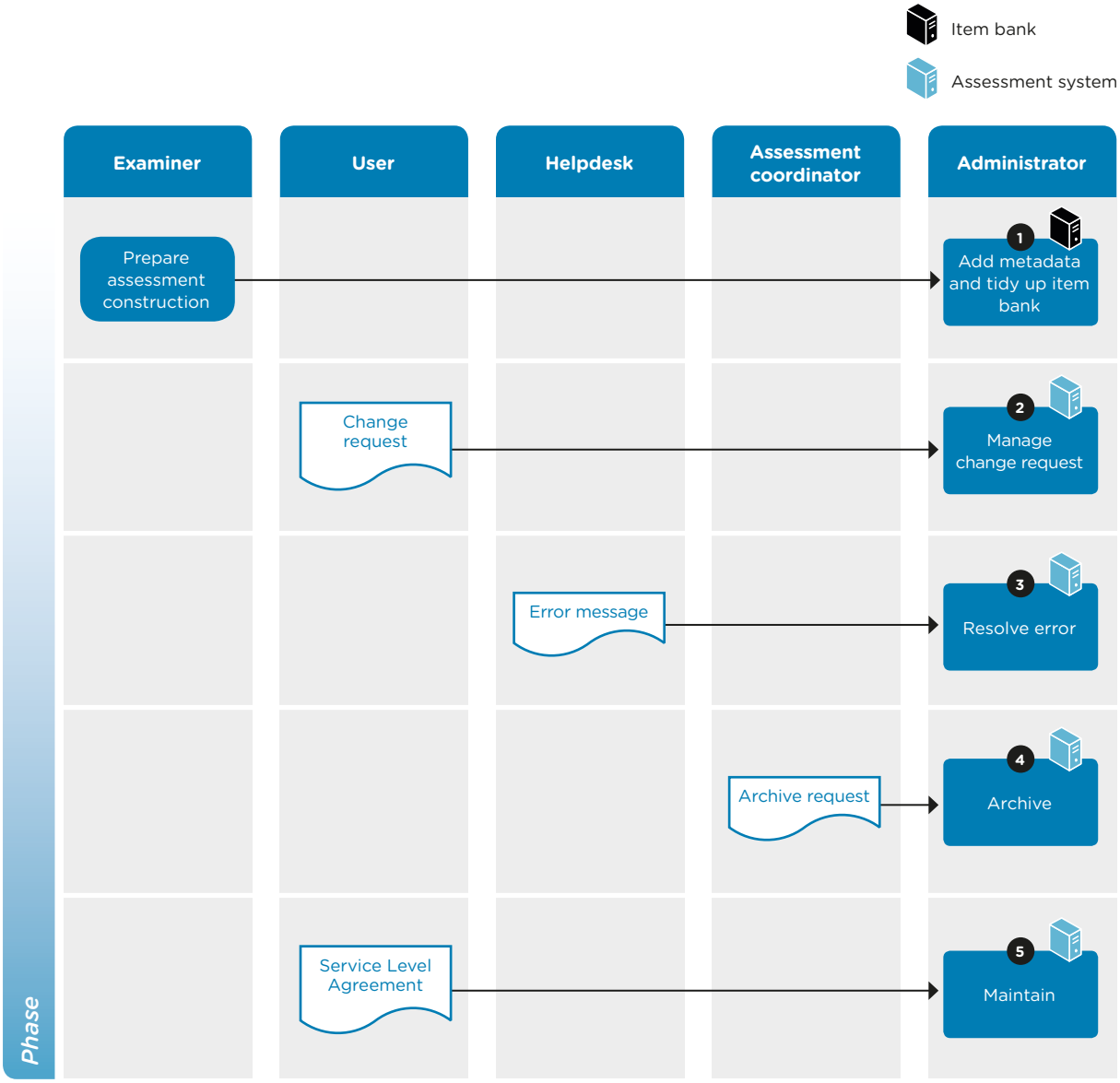
**Process description**
Technical, software and content management, maintenance and rejection of tools that are used in the assessment process.

**Process goal**
Maintenance of the assessment environment, including database/item bank, so that it remains suitable for the purpose for which it is used, and reliably archive assessments and assessment results.

**Process precondition(s)**
Process is reliable, efficient and effective.

**Input**
Objects to be managed, management agreements, requests for change and error messages.

**Output**
An assessment environment that is ready to use at the agreed times.



## ACTIVITIES IN SUB-PROCESS 8: MANAGE

| | Activity | How (procedural description) | When | Who |
|---|---|---|---|---|
| 1 | ADD METADATA AND TIDY UP ITEM BANK | The (data) manager cleans up the data in the item bank either regularly (such as per period or per year) or on demand. This means that used items can be learned from, metadata is added to new items, and outdated items are deleted from the item bank. | Throughout the year | Administrator |
| 2 | PROCESS CHANGE REQUEST | Change requests are recorded, evaluated for their urgency and impact, prioritised and then implemented (or not). Care is taken to test a change before it is brought into production. | | Administrator |
| 3 | RESOLVE ERROR | Messages are recorded, evaluated for their urgency, prioritised and then resolved and their status reported back to the person who reported it. | | Administrator |
| 4 | ARCHIVE | The data in the assessment database referred to in the archive request is copied to an external medium for storage for the required retention period (if there is one). | | Administrator |
| 5 | MAINTAIN | The pro-active installation – after prior testing – of new versions. Also the regular creation of backups (in line with the intervals agreed in the Service Level Agreement, such as daily or weekly). | | Administrator |

# RACI FOR THE WHOLE ASSESSMENT PROCESS

This table describes the roles and responsibilities for all those involved in the assessment process.

An explanation of the codes used:

- **R**esponsible: The person or department where the activity is performed.
- **A**ccountable: The person to whom the R needs to report or who ensures that the right decision is made. A person may in fact be both R and A if the specific task lies within their job description, and the person does not need to report on it directly.
- **C**onsulted: Any person who is consulted during the execution of the task.
- **I**nformed: Any person or system who/that is "informed" after the task is completed.

| Role | Main task/responsibility |
|---|---|
| APPLICATION ADMINISTRATOR | Responsible for the (more technically oriented) application management of the assessment system and reports to the assessment coordinator. |
| GRADES ADMINISTRATION | Entry and (as required) correction of grades (in the SIS). |
| EXAMINATION COMMITTEE | Responsible for ensuring the integrity of the assessment process. |
| EXAMINER (LECTURER/PEER) | Responsible for the assessment of the candidates' knowledge and skills. In terms of this process, more specifically: creating effective assessments and rating the answers. |
| FACILITIES EMPLOYEE | Responsible for (access to) the examination rooms, holding keys, setting up the room (not the assessment PCs) and possibly video monitoring. Reports to the assessment coordinator.<br><br>*NB: There are institutions where the facilities employee is assisted by a workplace manager or a rooms and locations manager. The facilities employee reports to the assessment coordinator.* |
| SOFTWARE ADMINISTRATOR | Responsible for the software administration of the assessment system and reports to the assessment coordinator. Serves as the link between the user organisation and the application manager/supplier. |
| COURSE/PROGRAMME MANAGER | Has final responsibility for the assessment process within his/her educational area. |
| PRINT SHOP | Responsible for making the requested number of copies of assessments. |
| STUDENT | Is involved as part of their learning process in assessments which measure the quality of skills and learning. |
| INVIGILATOR | Ensures that the assessment is held according to the rules. |
| TECHNICAL ADMINISTRATOR | Responsible for the technical management of servers and/or workplaces and reports to the assessment coordinator. |
| ASSESSMENT COMMITTEE | Monitors the educational quality of assessments. |
| ASSESSMENT COORDINATOR | Has ultimate responsibility for the examination process from the point of preparing the assessment (in consultation with the lecturer), the technology and the location through to when the invigilator arrives. The assessment coordinator can demonstrate that the assessment took place as required by law, and reports to the examinations committee.<br><br>*NB: The assessment coordinator can delegate his/her activities to an operational team.* |
| ASSESSMENT EXPERT | Advises on the quality of assessments, from their planning through to their evaluation. |

| No. | Activity | Assessment coordinator | Lecturer (Peer) | Technical administrator | Software administrator | Facilities employee | Invigilator | Assessment committee | Application | Examination committee | Student | Grade management |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | **Plan** | | | | | | | | | | | |
| 1 | Define assessment structure | | R | | | | | A | | | | |
| 2 | Define assessment matrix | | R | | | | | A | Item bank | | | |
| 3 | Review | | R | | | | | C | | A | | |
| 4 | Process feedback | | R | | | | | A | Item bank | | | |
| **2** | **Construct** | | | | | | | | | | | |
| 1 | Define assessment items | | R | | | | | A | | | | |
| 2 | Review assessment items | | R | | | | | C | Item bank | A | | |
| 3 | Process feedback | | RA | | | | | A | Item bank | | | |
| 4 | Confirm assessment | | C | | | | | | Item bank | RA | | |
| 5 | Compile assessment | | RA | | | | | | | | | |
| 6 | Review assessment | | RA | | | | | | | | | |
| 7 | Process feedback | | R | | | | | A | | | | |
| 8 | Review assessment | | A | | | | | R | | | | |
| 9 | Approve assessment | | I | | | | | | | R | | |
| 10 | Deliver assessment | | R | | | | | | | A | | |
| **3** | **Test administration – digitally** | | | | | | | | | | | |
| 1 | Prepare room for assessment | A | | | R | | | | Item bank | | | |
| 2 | Collect assessment details | RA | | | | | | | | | | |
| 3 | Prepare room | A | | R | | R | | | | | | |
| 4 | Release assessment | A | | | R | | | | Environment for taking examination | | | |
| 5 | Collect assessment details | A | | | | | R | | | | | |
| 6 | Open room | A | | R | | R | | | Work-stations | | | |
| 7 | Enter room | A | | | | | R | | | | | |

| No. | Activity | Assessment coordinator | Lecturer (Peer) | Technical administrator | Software administrator | Facilities employee | Invigilator | Assessment committee | Application | Examination committee | Student | Grade management |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | Enter room | A | | | | | | | | | R | |
| 9 | Make assessment available | A | | | | | R | | Environment for taking examination | | | |
| 10 | Take an assessment | | | | | | | | Environment for taking examination | | RA | |
| 11 | Close assessment | A | | | | | R | | Environment for taking examination | | | |
| 12 | Report progress | A | | | | | R | | | | | |
| **4** | **Test administration – on paper** | | | | | | | | | | | |
| 1 | Deliver assessment | A | R | | | | | | Item bank | | | |
| 2 | Receive | RA | | | | | | | | | | |
| 3 | Make copies centrally | | | | | R | | | Print shop | | | |
| 4 | Make copies locally | A | | | | R | | | | | | |
| 5 | Store | A | | | | R | | | Workstation | | | |
| 6 | Return | A | | | | R | | | | | | |
| 7 | Collect assessment with details | A | | | | | R | | | | | |
| 8 | Enter room | A | | | | | R | | | | | |
| 9 | Enter room | | | | | | | | | | RA | |
| 10 | Distribute assessment | A | | | | | R | | Environment for taking examination | | | |
| 11 | Take an assessment | | | | | | | | Environment for taking examination | | RA | |
| 12 | Collect assessment | A | | | | | R | | Environment for taking examination | | | |
| 13 | Report progress | A | | | | | R | | | | | |
| **5** | **Score** | | | | | | | | | | | |
| 1 | Make spare copy | A | | R | | | | | Environment for taking examination | | | |
| 2 | Collect answers to | RA | | | | | | | Item bank | | | |
| 3 | Score answers | | R | | | | | A | Item bank | | | |
| 4 | Second scoring | | R | | | | | A | Item bank | | | |
| 5 | Decide provisional grade | | R | | | | | | Item bank | A | | |

| No. | Activity | Assessment coordinator | Lecturer (Peer) | Technical administrator | Software administrator | Facilities employee | Invigilator | Assessment committee | Application | Examination committee | Student | Grade management |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **6** | **Analyse** | | | | | | | | | | | |
| 1 | Analyse answers | | R | | | | | | Analysis tool | A | | |
| 2 | Report analysis | | R | | | | | | Analysis tool | A | | |
| 3 | Determine assessment grade | | R | | | | | | Item bank | A | | |
| **7** | **Report** | | | | | | | | | | | |
| 1 | Enter grade | | R | | | | | | SIS | | | R |
| 2 | Import determine results | | R | | | | | | SIS | A | | |
| 3 | Consult grade | | | | | | | | SIS | | RA | |
| 4 | Offer view | | RA | | | | | | | | C | |
| 5 | Adjust grade | | RA | | | | | | SIS | | I | |
| 6 | Correct grade | | | | | | | | SIS | A | I | R |
| **7** | **Evaluate** | | | | | | | | | | | |
| 1 | Collect data | | R | | | | | | Item bank | | | |
| 2 | Interpret data | | R | | | | | | Item bank | | | |
| 2 | Draw conclusions | | R | | | | | | | | | |
| 3 | Record results | | R | | | | | | Item bank | | | |
| **8** | **Manage** | | | | | | | | | | | |
| 1 | Add metadata and tidy up Item bank | | R | | | | | | Item bank | | | |
| 2 | Handle change request | | | R | R | | | | Assessment system | | | |
| 3 | Resolve error | | | R | R | | | | Assessment system | | | |
| 4 | Archive | | | R | R | | | | Assessment system | | | |
| 5 | Maintain | | | R | R | | | | Assessment system | | | |

APPENDIX 2

# ASSESSMENT SECURITY ON THE BASIS OF BASELINE INFORMATION SECURITY

Higher education institutions in the SURF Community for Information Security and Privacy (SCIPR) have jointly defined a baseline in the area of information security. The full implementation of this baseline within the institution delivers generic information security at a medium level. The baseline is based on ISO 27002:2013, an internationally accepted set of standards.

The table below includes a very limited number of standards with examples of measures that apply specifically to the assessment process. The full baseline includes many other standards that are generic and also contribute to securing the assessment process at the medium level. Your institution's security officer can provide more information about this. We must emphasise that the assessment process can only be secured with maximum effect if the baseline is in order. This means that all measures required to meet the medium level need to have actually been implemented.

The measures specified in the table are "example measures". This means that a measure of this type is one possible approach to achieving the desired level of security. Other measures may also exist which can be implemented to achieve the same objective – we recommend always taking a critical approach to the example measures and evaluating how usable they are within the specific context of your own institution.

| ISO STANDARD | TEXT OF THE SECURITY REQUIREMENT (ISO 27002:2013) | EXAMPLE MEASURES ASSESSMENT PROCESS |
|---|---|---|
| 6.2.1.1 | **Policy for mobile equipment:** The policy and supporting security measures are defined in order to manage the risks involved when mobile equipment is used. | • The locations where work can be done on the assessment process are defined (for example, only in special rooms within the institution, only within the buildings of the institution, or "anywhere").<br>• There is an agreement on which tools (laptop, tablet and/or smartphone, personal equipment, only those devices belonging to the institution, etc.) may be used to work on the assessment process.<br>• Secure access to assessment data is achieved in a technical sense (depending on the location) by applying network and application security. |
| 7.2.2 | **Awareness, education and training about information security:** All employees of the organisation and, where relevant, contractors, are provided with suitable awareness training and regular refresh courses on the organisation's policy rules and procedures that are relevant for their work. | • Awareness campaigns (newsletters/ flyers) are held according to an annual programme.<br>• Assessment security is discussed regularly. |

| ISO STANDARD | TEXT OF THE SECURITY REQUIREMENT (ISO 27002:2013) | EXAMPLE MEASURES ASSESSMENT PROCESS |
|---|---|---|
| 9.1.1 | **Policy for securing access:** A policy for securing access is defined, documented and evaluated on the basis of the requirements for securing operations and information. | Applications and (mobile) users only receive the rights they actually need to carry out assessment-related tasks. |
| 9.2.1 | **Registration and removal of users:** A formal registration and cancellation procedure has been implemented to make it possible to assign access rights. | Assigning access rights for assessment software and data is done using a formal procedure, where possible automated via provisioning. |
| 9.2.6 | **Withdrawing or adjusting access rights:** The access rights for all employees and external users to information and information processing facilities are removed when their contract of employment, temporary contract or agreement ends, and are amended if the status of this contract/agreement changes. | In the assessment chain, each individual is restricted to the rights they need ("least privilege"). |
| 10.1.1.1 | **Policy on using encryption management rules:** To protect information, a policy has been developed and implemented for using encryption management rules. | Tools to enforce the policy in relation to the secure assessment process, such as secure apps and policies, are in place across the institution. |
| 13.2.1 | **Policy and procedures for transferring information:** Formal policy rules, procedures and management rules apply to transfers in order to protect the transfer of information that takes place using all kinds of communication channels. | • Using recognisable and sealed envelopes when sending assessments and assessment results.<br>• Sending examination script envelopes exclusively via a person who can be trusted.<br>• Tracking and tracing when transferring and sending |

APPENDIX 3

# SECURITY MEASURES PER SUB-PROCESS

The following tables list measures that contribute to a secure assessment process. These measures can be taken on top of the measures from the baseline for information security. These are recommended measures to reach a higher level of security than the medium level; they therefore apply mainly to aspects where the risk is high. Here, too, the measures listed should be looked at critically within the context of your own institution – there are other measures available that will achieve the same end.

### 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<br>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 | • Establishment of need-to-know access<br>• 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 | • Only required persons are granted read- and write-access<br>• 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. | • Track changes are visible<br>• Response to review is defined | Notification when track changes are processed |

| Activity | Integrity and confidentiality risks | | | | | Management measures | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Opportunity | Impact | | | setting up a system | authorisation (separation of duties) | reports | user controls |
| | | | I | C | | | | | |
| 4. Review assessment items | Unauthorised access to the assessment expert's workstation | M | M | H | | • Local storage only if encrypted, or storage in a (private) cloud<br>• Comments can only be made as comments or track changes | • Only required persons are granted read- and write-access<br>• Previous versions cannot be overwritten | Comments/proposed changes are visible | |
| | Interception of assessment or assessment items during transfer between workstations of those involved | H | M | H | | With two-factor authentication and encrypted connection to digital assessment environment | Only required persons are granted read- and write-access | Logging activities in digital assessment environment | Overview of login times, attempts and their IP addresses and users |
| 5. Confirm assessment items | Unauthorised access to the examiner's workstation | M | H | H | | Local storage only if encrypted, or storage in a (private) cloud | Access to PC with personal account only | Logging activities in digital assessment environment | Amendments and login behaviour are monitored |
| 6. Compile assessment | Unauthorised access to the examiner's workstation | L | M | H | | • Local storage only if encrypted, or storage in a (private) cloud<br>• Comments can only be made as comments (no track changes) | • Only required persons are granted read- and write-access<br>• Previous versions cannot be overwritten | Comments/proposed changes are visible | Status of assessment items is displayed |
| | Unauthorised access to author's environment | M | M | H | | With two-factor authentication and encrypted connection to digital assessment environment | Access to PC with personal account only | Comments/proposed changes are visible | |
| 7. Review assessment | Unauthorised access to the reviewer's workstation | M | M | H | | • Local storage only if encrypted, or storage in a (private) cloud<br>• Comments can only be made as comments or track changes | • Only required persons have read- and write-access<br>• Previous versions cannot be overwritten | Comment/proposed changes are visible | Number of comments is displayed |
| | Interception of assessment items during transfer from examiner's workstation to shared environment | M | M | H | | With two-factor authentication and encrypted connection to digital assessment environment | Only required persons are granted read- and write-access | Logging activities in digital assessment environment | Overview of login times, attempts and relevant IP addresses |
| 8. Process feedback | Unauthorised access to the examiner's workstation | M | H | H | | Local storage only if encrypted, or storage in a (private) cloud | Only assessment owner (examiner) has right to accept track changes | Track changes are visible | Notification when track changes are processed |
| 9. Review assessment | Unauthorised access to the reviewer's workstation | M | H | H | | • Local storage only if encrypted, or storage in a (private) cloud<br>• Comments can only be made as comments or track changes | • Only required persons have read- and write-access<br>• Previous versions cannot be overwritten | Comment/proposed changes are visible | Number of comments is displayed |
| | Interception of assessment items during transfer from examiner's workstation to shared environment | M | M | H | | With two-factor authentication and encrypted connection to digital assessment environment | Only required persons are granted read- and write-access | Logging activities in digital assessment environment | Overview of login times, attempts and their IP addresses |
| 10. Approve assessment | Unauthorised access to the examiner's workstation | M | H | H | | Only working in secured shared environment | Only required persons are granted read- and write-access | Logging activities in digital assessment environment | Overview of login times, attempts and their IP addresses |
| 11a. Digital delivery of assessment | Interception of assessment items during transfer from examiner's workstation to shared environment | H | H | H | | With two-factor authentication and encrypted connection to digital assessment environment | Only required persons are granted read- and write-access | Logging activities in digital assessment environment | Overview of login times, attempts and their IP addresses |
| 11b. Delivery of assessment on paper/ receipt of assessment | Unauthorised viewing of questions or standardisation or unauthorised change to standardisation. | H | M | H | | • Print only in controlled access rooms, and print securely<br>• Process prints (sort/pack/ store, etc.) in controlled access rooms only | Envelopes are sealed by sender | Define times of transfers (Track & Trace) | Examiner can see what stage of the duplication/transfer process the assessment has reached |

### 1.3. Test adminstration

The environment in which summative assessment is carried out digitally is subject to relatively high risk. As institutions already apply many measures in this area, the items in the table therefore focus on digital examinations, a relatively new field.

| Integrity and confidentiality risks | | | | | Management measures | | | |
|---|---|---|---|---|---|---|---|---|
| | Opportunity | Impact | | | setting up a system | authorisation (separation of duties) | reports | user controls |
| | | I | C | | | | | |
| Tampering with assessment software potentially resulting in fraud | M | H | H | | Securing assessment software through:<br>• Time-limited availability<br>• Location-limited availability | • Access only for those who are explicitly authorised<br>• Access with minimum rights | Logging access to server and application | • Regular installation of updates and patches<br>• Regular security audit<br>• Monitoring of logs after examination has been sat<br>• Server and network component hardening<br>• Taking tips from students seriously |
| Tampering with examination PCs prior to the assessment | M | H | H | | • Examination rooms with special locks so that difference to standard locks is evident<br>• PCs for administering tests are updated daily with authentic programmes (images)<br>• Input ports if USB not ready or missing<br>• Set up PCs on tables in examination rooms that are physically enclosed | | Logging of imaging procedure | • Provision of extra secure key<br>• Daily monitoring of imaging process |
| Work can be performed on the assessment before/after assessment is completed | M | H | H | | • Logging at start and end of each assessment<br>• One-time only assessment start-up possible (emergency procedure available for exceptions) | | | Monitoring of logins after assessment is complete |
| Examination PC has been tampered with; unable to determine who was responsible | L | H | H | | • Log which student has been working on which PC<br>• Assign a PC to each student | | Usage log | • Check user list<br>• Check video surveillance images |

Risks and measures per activity:

| Activity | Integrity and confidentiality risks | | | | Management measures | | | |
|---|---|---|---|---|---|---|---|---|
| | | Opportunity | Impact | | setting up a system | authorisation (separation of duties) | reports | user controls |
| | | | I | C | | | | |
| 1. Prepare room for assessment | Assessment is made available too early (or too late) in the examination environment | M | L | M | Preparation carried out using pre-programmed steps | • Access only for those who are explicitly authorised<br>• Access with minimum rights | | Prepare only after authorised request received, or apply four-eyes principle |
| 2. Collect assessment details | Unauthorised access to the assessment coordinator's workstation | L | H | H | See Planning sub-process | | | |
| 3. Prepare room | Tampering with workstations in the examination room such as hardware key-loggers | H | H | H | Rooms locked at all times except during examinations | Access only for designated room managers outside assessment times | | • Monitoring access to room using cameras, registrations and strict access management using key or pass card<br>• Room manager physically checks connections and components |

| Activity | Integrity and confidentiality risks | | | | | Management measures | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Opportunity | Impact | | | setting up a system | authorisation (separation of duties) | reports | user controls |
| | | | I | C | | | | | |
| 4. Release assessment | Assessment questions are revealed too early | L | H | H | | Separate release of assessment and release to those administering it | Only released by Software administration role | | Only released following authorised request |
| 5. Collect assessment details | Interception of details during transfer between the workstations or workplace of invigilator and assessment coordinator | M | M | M | | See Planning sub-process | | | |
| | Tampering with assessment details (especially: adding name to list of participants) | M | M | M | | | | | Assessment details transferred in sealed envelope |
| 6. Open room | Room is opened too early, meaning that room can be tampered with | L | M | L | | | Key is only released to previously identified assessment supervisors | Record key handover in log | Key to room is available from one hour before examination starts |
| 7. Access to room (invigilator) | | | | | | | | Record entry time in the minutes | |
| 8. Access to room (student) | | | | | | | Access permitted only for students registered for examination (e.g. after scanning college card) | | Access from 15 minutes before start, checked by invigilator |
| 9. Make assessment available | Assessment questions are revealed too early | M | L | H | | Available no more than 10 minutes before start | | Record time of provision of questions in the minutes | |
| 10. Take an assessment | It is not the student him/herself who takes the assessment, but a substitute | H | H | H | | Display on-screen a photo of the registered student in the assessment system | | | Identity checked by invigilator |
| | Take assessment without being registered for it | H | H | H | | Assessment can only be started if account is activated | | | Invigilator checks registration |
| | Viewing files and public distribution during the assessment | H | H | H | | Block internet and network access (e.g. by locking down browser), including if using students' laptop (secured BYOD solution) | | | Invigilator checks that no private items are taken into the examination room |
| | Unauthorised collaboration and/or querying files | H | H | H | | • Secure set-up for workstations (distance apart) and protection of screens (partitions, privacy filters)<br>• Randomising questions | | | • Supervision by invigilator while examination is underway<br>• Reports from students and invigilators (during or after an examination) about fraud are taken seriously |
| | The assessment can be restarted multiple times by a student to allow answers to be corrected, etc. | M | H | H | | Programme in advance how often the assessment can be taken by a student | | | |
| | Use of crib sheets and similar | H | H | H | | | | | Supervision by invigilator while examination is underway |
| | Visiting toilets | H | H | H | | • Only allow access to toilet areas during examinations<br>• Check toilet areas before examinations | | | Visit to toilet accompanied by invigilator |
| 11. Close assessment | Assessment available for too long, meaning candidates have access to it for too long | M | H | M | | Assessment is closed automatically | | Record time of closure in minutes | |
| 12. Report progress | Assessment material not controlled during reporting | M | H | H | | | | | Store documents in sealed envelope, box, etc. |

### 1.4. Scoring

See the sub-process relating to paper and digital assessments. The table below has been completed for both types.

| Activity | Integrity and confidentiality risks | | | | | Management measures | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Opportunity | Impact | | | setting up a system | authorisation (separation of duties) | reports | user controls |
| | | | I | C | | | | | |
| 1a. Make a back-up | Back-up is incomplete or unusable | M | H | H | | • Automatic message in the event of technical errors<br>• Set up automatic back-up | Full read-only rights for back-up account | Status report | • Initial test that is working correctly<br>• Regular check that back-up is usable |
| 1b. Digitise paper-based assessment | Not all pages completed | H | M | L | | • Automatic metadata<br>• Store in secure environment | Digitaliseren alleen door geautoriseerd persoon | Digitisation report | All assessments and pages present in digital form and legible. |
| 2. Collect answers | Not all answers (of completed assessments) were collected | M | H | L | | All completed assessments are stored together (one envelope and/or folder). For digital assessments store as read-only. | | | Check match of who was present against name on assessments |
| | Unauthorised person collects answers or changes answers | M | H | H | | • Digital: Two-factor authentication when logging in<br>• Paper: identification when collecting | Only persons assigned to assessment can collect assessments | Note (log) by whom and when an assessment is collected | Check identity of person who collects |
| 3. Score answers | Unauthorised access to examiner's workstation | M | H | H | | Local storage only if encrypted or view in (private) cloud<br>Digital: Two-factor authentication | For digitally created work read-only rights | Corrections visible as comments (digital) or in different colour pen (paper) | |
| 4. Second scoring | Unauthorised access to examiner's workstation (2nd corrector) | M | H | H | | As above | | | |
| 5. Decide grade | Use of incorrect pass mark (standardisation set) | L | H | L | | Version management on standardisation set | | Tampering report on standardisation set | Calculation checked by peer |

### 1.5. Analysis

Analysis identifies items that were poor quality, for example because they appear to be too easy, too difficult or ambiguous The replies are copied to the analysis environment, e.g. a statistics programme. The analysis may lead to a revision of the standardisation and therefore to an adjustment of the grades.

| Activity | Integrity and confidentiality risks | | | | | Management measures | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Opportunity | Impact | | | setting up a system | authorisation (separation of duties) | reports | user controls |
| | | | I | C | | | | | |
| 1. Analyse answers | Unauthorised access to assessment expert's workstation | M | H | H | | • Local storage only encrypted or analysed in the read-only (private) cloud<br>• Access to answers uses two-factor authentication | Answers cannot be changed, using read-only option | | |
| | Unauthorised access to analysis environment | L | H | H | | Access to the analysis environment uses two-factor authentication | Answers cannot be changed, using read-only option | | |
| 2. Report analysis | Tampering with grades on transfer between item bank/examination environment and analysis | M | H | H | | Automatically encrypted transmission by applying server certificate | | | For web-based access security is displayed using a green padlock in the browser's address bar |
| 3. Determine grades | Unauthorised access to examiner's workstation | M | H | H | | Access to grades in the item bank using two-factor authentication only | Access to workstation through personal account only | Logging activities in the item bank | Final check on the audit trail: revision only by authorised user(s) |

### 1.6. Reporting

Reporting covers publication, viewing and determination grades in, for example, the student information system (SIS). There are a number of risks that need to be identified here, such as unauthorised changes to grades.

| Activity | Integrity and confidentiality risks | | | | | Management measures | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Opportunity | Impact | | | setting up a system | authorisation (separation of duties) | reports | user controls |
| | | | I | C | | | | | |
| 1. Entry of grades | Tampering with examination results slips | L | H | M | | Digitising examination results slips | | | • Hand in personally<br>• Secured storage |
| | Typing error on entry | M | H | M | | • Check permitted grade formats<br>• Check if assessment is active | Entry only by examiner and administration (on behalf of examiner) | Regular monitoring of statement of changes | Approval of grade by examiner/ third party |
| 2. Import/determine results | Incorrect upload | M | H | M | | • Upload programme tested in advance<br>• Checks during upload, such as: course code on slip and file are the same | Rights according to authorisation matrix | Transaction report | • Compare grades provided and uploaded<br>• Transaction report with no omissions |
| | Determined incorrectly | M | H | L | | | Grade determination only available to examiner | Transaction report | Compare entries to source document |
| | Tampering with grades on transfer from examiner to SIS (digital, via network) | L | H | H | | Send results with encryption | | | |
| 3. View grade (student) | Viewing by someone other than student | M | L | M | | • Access to own results only<br>• Other access according to authorisation matrix | | Authorisation report | Regular checks on assigned authorisations compared to authorisation matrix |
| | Consult invalid grades | M | L | M | | Only approved grades can be consulted | Approved by examiner | | |
| 4. Offer view | Unauthorised access to submitted work | M | H | H | | | Can only view own material | Define access (who, when) | When not visible, secure storage |
| | Unauthorised changes to submitted work | M | H | H | | Digital view: read-only rights | | | View under supervision |
| 5. Adjust grade | Put examiner under pressure | L | H | H | | Adjustments using two-factor authentication only | Can only be adjusted by administration after approval by examinations committee or examiner | Change report including reason for changes | |
| | Unauthorised changes from examiner's workstation | M | H | H | | | | Change report | Weekly check of change report |
| | | | | | | | | | Report back adjustment |
| 6. Correct grade | Unauthorised access to a grade administrator's workstation | M | H | H | | | Adjustments only allowed by administration | Change report | Weekly check of change report |
| | Tampering with appeal decisions | L | H | H | | Digital signature on decisions | | | Report back adjustment |
| | Tampering with grades in the SIS | M | H | H | | Increased security in SIS | | Report before and after | Monthly check on timing of amendments |

### 1.7. Evaluation

In the evaluation sub-process, the quality of the various items and the assessment as a whole are evaluated on the basis of past/completed assessments with the aim of achieving better evaluations, assessment items and/or assessment matrices. Given that between evaluation and reuse there is a period of revision and potentially recovery available, there is no major risk during the evaluation part of the process.

| Activity | Integrity and confidentiality risks | | | | | Management measures | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Opportunity | Impact | | | setting up a system | authorisation (separation of duties) | reports | user controls |
| | | | I | C | | | | | |
| 1. Collect data | | M | M | M | | | Only those involved in the evaluation have read-only access to the data | | |
| 2. Interpreting information | Unauthorised access to information | M | M | M | | | | | |
| 3. Draw conclusions | | M | M | M | | | | | |
| 4. Record results | Unauthorised access to the item bank | M | M | M | | Access to the grades in the item bank only with two-factor authentication | Access to the item bank only with personal account and only to the relevant parts | Logging activities in the item bank | Final check on the audit trail: access for authorised user(s) only |

### 1.8. Managing

The management of assessments and assessment results is always focused on being able to justify the results afterwards, and the potential reuse of assessment items and assessments.

| Activity | Integrity and confidentiality risks | | | | | Management measures | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Opportunity | Impact | | | setting up a system | authorisation (separation of duties) | reports | user controls |
| | | | I | C | | | | | |
| 1. Add metadata and tidy up item bank | Metadata added incorrectly | M | M | L | | • Programmed entry validation<br>• Using fixed selection lists | Metadata added by trained expert | Report of amendments | Quality checked by peer |
| | Incorrect items deleted | M | M | L | | Logging of deleted items | Expert only has access to own items | Report of amendments | Quality checked by peer |
| | Items are corrupted | M | M | L | | Logging of items before and after changes | Expert only has access to own items | Report of amendments | Quality checked by peer |
| | Account management being abused | L | H | H | | Baseline plus two-factor authentication | | | Regular check of amendments |
| 2. Handling requests for amendment | Amendment introduces error | M | H | H | | Install version management | | Test report | • Perform acceptance test<br>• Amendment into production after agreement by process owner |
| 3. Resolve error | Solution introduces error | M | H | H | | Install version management | | Test report | • Perform acceptance test<br>• Amendment into production after agreement by process owner |
| | Items are not secure while error exists | L | H | H | | • Failsafe device<br>• Automatic message if component stops | | | |
| 4. Archive | Archive is incomplete | M | H | L | | | Full read-only access to archive account | Status report | Check by archive manager |
| | Archive is unusable | M | H | L | | Automatic message on technical error | | | Regular check of accessibility by reading out archive |
| | Unauthorised access to archive | M | L | H | | • Access controls<br>• Encryption of archive | Only employees working with archive have access | Access list | • Check keys<br>• Monthly log check |

| Activity | Integrity and confidentiality risks | | | | | Management measures | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | Opportunity | Impact | | | setting up a system | authorisation (separation of duties) | reports | user controls |
| | | | I | C | | | | | |
| 5. Maintain | New version includes errors | M | H | H | | Install version management | | Test report | • Perform acceptance test<br>• Amendment into production after agreement by process owner |
| | Back-up is incomplete or unusable | M | H | L | | • Automatic message on technical error<br>• Set up automatic back-up | Full read-only access to back-up account | Status report | • One-time installation test<br>• Regular check that back-up is usable |
| | Unauthorised access to archive | M | L | H | | Access controls | Only employees working with archive have access | • Access list<br>• List of examination scripts to be deleted | • Check keys<br>• Monthly log check |

APPENDIX 4

# REVIEW OF SECURE ASSESSMENT

The international standard ISO 27002:2013 describes in chapters five to eighteen the aspects relating to information security that need to be complied with for good practice. All security officers in higher education apply this good practice within their institutions, which is why also applying this standard within the assessment process is such a practical approach.

The matrix below shows the chapters with their associated requirements entered for the assessment process. You are recommended to use this matrix as an initial measure, and then repeat the evaluation of the level of security on an annual basis. We recommend that you work on this with the security officer for your institution. Based on this matrix, you can decide whether the assessment process is adequately secured. You can have an external audit carried out, or you can perform a self-assessment. Note: this table includes more than just the measures that apply specifically to the assessment process, as stated in Chapter 2 of this workbook.

| Ch. | Effect/selection of relevant requirements from ISO standard |
|---|---|
| 5. | **Assessment policy:**<br>1. Institution has created an assessment policy including at a minimum a goal, responsibilities and (regular) compliance checks.<br>2. The assessment policy is available to those affected, including in the Course and examination regulations and in the form of practical instructions, and is regularly brought to their attention. |
| 6. | **Organising a secure assessment process:**<br>1. The roles within the assessment chain are clearly defined and communicated.<br>2. The locations where activities are permitted to be performed for the assessment process (at home, examination room, BYOD) are defined in clear detail. |
| 7. | **Secure personnel (such as lecturers, IT managers, invigilators and assistants):**<br>1. The persons who may be employed and the conditions of their employment during the assessment process are set out.<br>2. The knowledge/experience that each person needs to have is set out.<br>3. Training or training materials are available.<br>4. Current confidentiality statement (or equivalent) has been signed. |
| 8. | **Managing business assets:**<br>1. The assets used within the assessment process (including the owner and manager) are set out.<br>2. It is clear what level of confidentiality applies to each part of an assessment (questions, pass mark, formative, summative, etc.).<br>3. The handling of removable media (CDs, USB sticks, paper) is set out. |
| 9. | **Securing access:**<br>1. The persons who have access to assessment equipment are defined, as are the places and times.<br>2. Access to the network and application(s) is secured at all times throughout the entire assessment process.<br>3. Access rights for all kinds of users are defined (accounts, validity, options within accounts).<br>4. In particular, special access rights for managers and coordinators are properly defined.<br>5. Access rights are regularly analysed and adjusted/withdrawn where necessary.<br>6. Users are familiar with the way in which passwords and similar need to be handled.<br>7. Passwords are managed reliably.<br>8. Where necessary, secure login procedures apply (double logins, strong authentication, such as using SURFconext).<br>9. Access to source code (such as for the assessment program) is properly controlled. |

| | |
|---|---|
| 10. | **Encryption:**<br>1. The parts of the assessment process subject to encryption are defined.<br>2. Management of the encryption keys is properly organised. |
| 11. | **Physical security and securing the environment:**<br>1. The locations (rooms) which are secured for the assessment process are defined.<br>2. The physical security setup is defined<br>3. The manner of access (and the records of access) to the secured rooms is defined.<br>4. The setting up (e.g. privacy screen filter or similar) and placement (space between assessment PCs, partitions) of equipment used in the secured rooms are defined.<br>5. The persons who can perform maintenance and the measures/tools are defined.<br>6. The items (paper, equipment) that can be taken out of the secured rooms are defined. |
| 12. | **Security management:**<br>1. The way in which the tools used in the assessment process may be used is defined.<br>2. The way in which tools (assessments, answers, applications, systems) may be amended is defined.<br>3. The manner in which it is ensured that equipment provides adequate capacity is defined.<br>4. Separation of development, test and production environments is in place.<br>5. Environments and equipment are protected from malware.<br>6. Back-ups are made of assessment materials and results.<br>7. Relevant assessment activities are logged.<br>8. Logs are also properly protected.<br>9. Times in the various logs (and systems) are synchronised.<br>10.The integrity of systems within the assessment process is guaranteed.<br>11. Protection is provided against technical vulnerabilities (hardening, virus scanners). |
| 13. | **Securing communications during the assessment process:**<br>1. The network and network services are managed.<br>2. The network and network services are secured, e.g. by separating networks.<br>3. Messages are exchanged with adequate security. |
| 14. | **Acquisition, development and maintenance of applications:**<br>1. Requirements are defined for systems and applications (both during development and management).<br>2. Requirements are agreed with suppliers (internal/external).<br>3. Checks are performed on compliance with agreed requirements.<br>4. Tests are carried out on (new, amended) applications before they are used. |
| 15. | **Supplier relationships:**<br>1. Secure access by suppliers is defined both formally and in practice.<br>2. Wherever a supplier chain exists, access is defined within the chain.<br>3. Compliance with supplier agreements is monitored. |
| 16. | **Managing incidents:**<br>1. The roles and responsibilities that currently apply in relation to assessment incidents are defined.<br>2. Incidents are reported.<br>3. Reporting of potential weak points in the security for the assessment process is organised.<br>4. Incidents are evaluated and handled correctly.<br>5. We learn from incidents.<br>6. In the event of incidents, evidence is collected in a structure manner. |
| 17. | **Assessment continuity:**<br>1. Continuity plans exist, are up to date and are tested regularly.<br>2. Where necessary, redundant components are available. |
| 18. | **Compliance:**<br>1. Legal, contractual and policy requirements are complied with. This includes requirements relating to archiving and intellectual property.<br>2. Protection of privacy for those involved (especially those taking the assessments) is correctly organised.<br>3. Compliance with requirements relating to the secure assessment process is guaranteed through independent inspections. |

APPENDIX 5

# HORA OBJECTS INVOLVED IN THE ASSESSMENT PROCESS

The Higher Education Reference Architecture (Hoger Onderwijs Referentie Architectuur, HORA), defines a large number of business objects[6]. These are elements that are relevant from an operational perspective. The HORA architecture team has created a proposed classification for these business objects, relating to the required quality levels for availability, integrity and confidentiality. The business objects that are involved in the assessment process are listed below. This classification is also used to determine their classification within the sub-processes, including in the risk matrix in Chapter 2 and the security measures in Appendix 3.

| HORA OBJECTS INVOLVED IN THE ASSESSMENT PROCESS | | | |
|---|---|---|---|
| Object | Availability | Integrity | Confidentiality |
| Degree programme | Medium | High | Public |
| Curriculum | Medium | High | Low |
| Examination programme | Medium | High | Low |
| Assessment result | Low | High | Medium |
| Educational unit result | Low | High | Medium |
| Education agreement | Low | Medium | Low |
| Participant | Medium | High | High |
| Security document | Low | High | Low |
| Class | Medium | Medium | Low |
| Learning group | Low | Medium | Low |
| Skill | Low | Low | Public |
| Learning activity | Medium | Medium | Low |
| Participant activity | Medium | Medium | High |
| Evaluation | Low | High | Medium |
| Schedule | High | Medium | Low |
| Assessment material | High | High | High |

[6] http://www.wikixl.nl/wiki/hora/index.php/Categorie:Bedrijfsobjecten

APPENDIX 6

# SOURCE MATERIAL USED


- Digital test terminology (SURF/Michiel van Geloven, 2013) https://www.surf.nl/en/knowledge-base/2013/digital-test-terminology.html

- Guidelines for Secure digital assessment [Richtsnoer Veilige digitale toetsafname] (SURF, v2.0 May 2014) ref 19.735, 2014) (in Dutch) https://www.surf.nl/kennisbank/2013/richtsnoer-veilige-digitale-toetsafname.html

- Process Description of Testing and Assessment by VHL college, partially based on process description drawn up by Saxion [*Procesbeschrijving Toetsing en Beoordeling door hogeschool VHL, mede gebaseerd op procesbeschrijving van Saxion*]. (internal document)

- Success! A Helping Hand for Exam Boards [*Geslaagd! Handreiking examencommissies*] (HBO council of the association of technical universities [raad vereniging van hogescholen], February 2011)

- Information security model from the Higher Education Security Model Framework [*Model beveiligingsbeleid uit het Framework Informatiebeveiliging Hoger Onderwijs*] (SCIPR, May 2015) https://www.surf.nl/binaries/content/assets/surf/nl/2015/informatiebeveiligingsbeleid-xx-v20-2015.pdf

- Baseline for information security in Higher Education v1.0 [*HO Baseline informatiebeveiliging v1.0*] (SCIPR, 1 May 2015) (in Dutch) https://www.surf.nl/binaries/content/assets/surf/nl/2015/baseline-informatiebeveiliging-ho-2015.pdf

# ACKNOWLEDGEMENTS

**Project management and content preparation**
Jenny de Werk, *SURFnet*
Michiel van Geloven, *SURFnet*
Martin Romijn, *SURFnet*

**Core group for secure assessment**
Monica Buijinck, *Saxion University of Applied Sciences*
Roger Deimann, *Amsterdam University of Applied Sciences*
Louwarnoud van der Duim, *National University Groningen*
Ludo van Meeuwen, *Eindhoven University of Technology*
Lud Overkamp, *Saxion University of Applied Sciences*
Nils Siemens, *Amsterdam University of Applied Sciences*
Hans van der Wal, *Saxion University of Applied Sciences*
Dorinde Winkelaar, *The Hague University of Applied Sciences*
Alwin Wullink, *Saxion University of Applied Sciences*

**Sounding board group of security officers**
**(SURF community for information security and privacy, SCIPR)**
Bart van den Heuvel, *Maastricht University*
Elma Middel, *Hanze University of Applied Sciences*
Martijn Plijnaer, *Inholland University of Applied Sciences*
Anita Polderdijk-Rijntjes, *Windesheim University of Applied Sciences*
Alf Moens, *SURFnet*

**Sounding board group of assessment experts**
Joost Dijkstra, *Maastricht University*
Meta Keijzer-de Ruijter, *Delft University of Technology*

**Layout**
Vrije Stijl, Utrecht

**Cover photograph**
Flickr - www.flickr.com/photos/yusamoilov/13334048894

April 2017

**SURFnet**

Moreelsepark 48
3511 EP Utrecht

PO box 19035
3501 DA Utrecht

+31 (0)88 787 30 00
www.surf.nl/surfnet