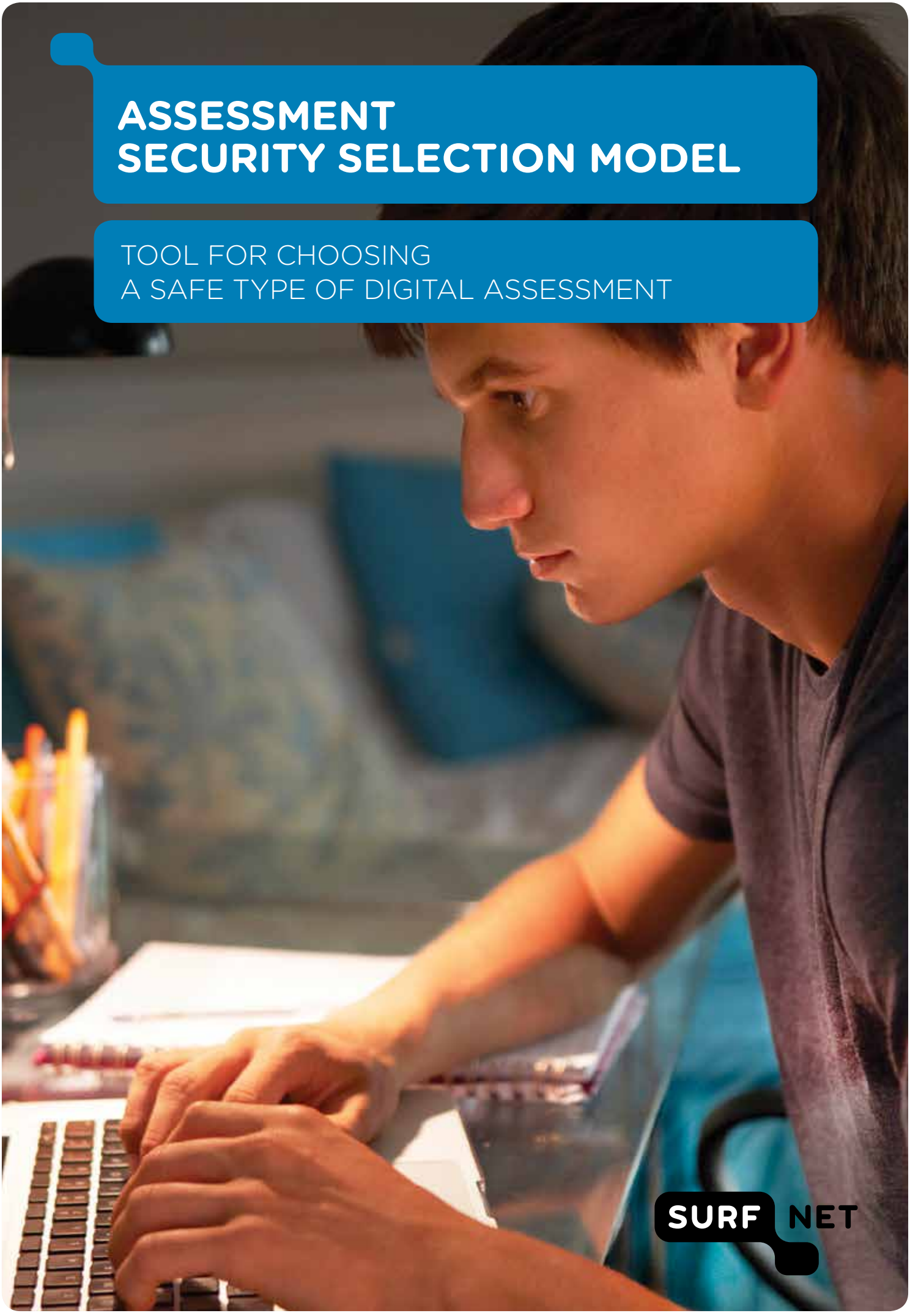
# ASSESSMENT SECURITY SELECTION MODEL

TOOL FOR CHOOSING
A SAFE TYPE OF DIGITAL ASSESSMENT



SURF NET

# ASSESSMENT SECURITY SELECTION MODEL

**With more and more digital assessment options coming at hand, we see that examination committees, policy makers and other parties are wrestling with the issue of which type of assessment provides the best security in a particular situation. When should you use online proctoring? When should you opt for 'bring your own device (BYOD)'? When is a computer room the best option?**

To decide on a suitable method for digital assessment, we usually look at the level of risk (the 'stakes') involved in a specific exam first and foremost. Frequently, a distinction is only made between two levels: high stakes and low stakes. This approach ignores many nuances:

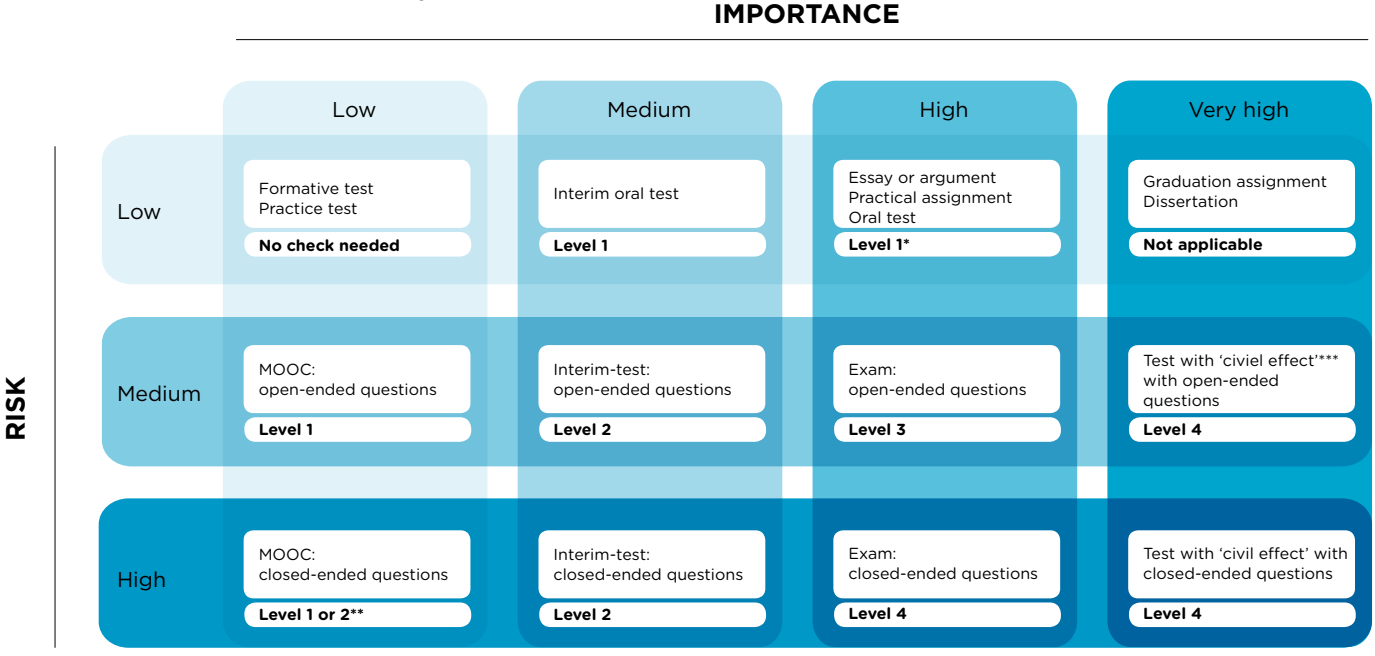
1. All summative exams (including both interim tests and final exams) are regarded as high-stakes exams.
2. No distinction is made based on the assessment format (multiple choice, oral exam or essay) despite the fact that this has a major impact on the suitability of different assessment methods. This is because the risk of fraud is much greater with multiple choice tests than in an oral exam.

To facilitate a more reasoned decision-making process, SURFnet has developed a model in which both the risk of fraud and the importance of the exam result are taken into account. This model offers examination boards guidelines for determining whether the intended assessment situation is adequate, and to ascertain which assessment methods would be suitable within the curriculum.

## The selection model

The selection model is based on classification by risk and importance. Below, the model has been partially completed to illustrate how it can be used. Each examination board can adapt it to their own context. When doing so, they should also take into account the context of the curriculum. For example, if certain knowledge is assessed multiple times during a study programme, the examination board may attach less importance to an earlier test than to a later test. After all, the knowledge would be retested and a student committing fraud would then find themselves caught out.
The model indicates the corresponding security level for each combination of importance and risk. This may mean, for instance, that a selection is made between different forms of online proctoring, or that a decision is made between BYOD and a fixed configuration for digital assessment.

### Assessment security selection model




* Naturally, online proctoring is unsuitable for essays and work performed over long periods of time. It is particularly suited to oral exams, for example.
** For MOOCs, this depends on the value placed on the MOOC.
*** For instance, authorisation to enter professional practice as a solicitor or in the judicial system.

# THE BASIS OF THE SELECTION MODEL IS A CLASSIFICATION BY RISK AND IMPORTANCE

## Importance of the exam

The selection model identifies four levels to indicate the importance of an exam:

- *Low*
  These are formative exams or online courses with no great social value attached. This might include MOOCs, such as courses by Coursera or programmes offered by the Universiteit van Nederland.
- *Medium*
  At this level, the exams do not directly contribute (significantly) to the transcript, but there are still consequences attached to them. Examples include small weekly interim tests that together might result in an extra point, or tests that give access to a module, an exam or an internship.
- *High*
  These are exams that have a direct and significant impact on the student's study credits. This will apply to all exams for modules that attract study credits, but also for partial examinations that together contribute towards the final assessment.
- *Very high*
  This category includes specific modules or tests which demand higher fraud prevention standards due to the nature of the courses or certain[1] (legal) consequences, such as assessments that would then allow you to work as a solicitor or in the judicial system (civil effect) or assessments for attaining BIG registration[2]. It may also include exams that are important for other reasons, such as the CITO exam, final exams in secondary schools or language and maths tests for PABO (basic teacher training).

## Fraud risk

The selection model identifies three levels to indicate the risk of fraud in relation to a particular exam:

- *Low*
  This is an exam where the student submits an entirely unique work, such as a thesis, essay or practical assignment, or completes an oral exam. In these cases, fraud prevention focuses on detecting plagiarism and establishing that the student has actually completed the work themselves.
- *Medium*
  An exam requiring unique answers, but which is not entirely the student's own work (as with a thesis or essay). This may be a written test with open-ended questions, where the answers are of sufficient length to be unique to each student. This might be a test requiring advanced mathematical calculations on paper, or where answers have to be substantiated with several lines of text.
- *High*
  Exams in which only a single answer is possible, and in which students do not – in the majority of cases – give unique answers. This includes all closed-ended questions, including multiple choice.

1. These may be requirements imposed by the examination board, but may also ensue from the general wishes of society at large or from legislation and regulations. The ultimate assessment, however, will always be made by the examination board.
2. The register of professionals working in the Dutch healthcare sector. Only registered persons are authorised to practise their professions. See also: https://www.bigregister.nl/en/

# THE SECURITY REQUIREMENTS PARTLY DEPEND ON THE TYPE OF ASSESSMENT

## Level classification by assessment method

Classification by levels of the different types of digital assessment method (BYOD, online proctoring and computer rooms) is set out below. The following two observations apply:

1. The classification has been determined on the basis of the type of system (e.g. two cameras for online proctoring or a dedicated assessment client) rather than on the practical application of the system. If a solution is poorly implemented (e.g. because it is easy to hack), the method will not be secure. This model is a tool intended to help you find a suitable model, not to help you choose an exact solution or supplier.
2. Traditional assessment rooms are not included because each examination committee can make its own estimation as to the level of security of the assessment room. This model only includes digital assessment methods.

### Online proctoring (outside the institution)

Online proctoring is inherently insufficient in its level of security for level 4 assessments.[3] Using extra cameras and logging makes the system more reliable.

- level 1: screen capture and a single camera
- level 2: screen capture and two cameras
- level 3: full logging, screen capture, two cameras (live proctoring or a recording only[4])
- level 4: online proctoring is unsuitable for level 4

### Bring your own device to an assessment room at the institution

The basic assumption of BYOD is that the earlier security measures are enforced in the booting process, the more secure the solution becomes.

- level 1: on the basis of a personal log-in process, in a controlled environment
- level 2: locked browser
- level 3: a secure client
- level 4: bootable assessment environment (both USB and network)[5]

### Digital assessment room at the institution with computers belonging to the institution

The basic assumption is that a digital assessment room with computers at the institution (and supervisors) already provides a reasonable level of security. A good secure client and, for example, and a basic form of proctoring[6] provide a higher level of fraud-proofing.

- level 1 and 2: not protected, but with a personal log-in process and surveillance
- level 3: secure client in combination with whitelists (if using internet)
- level 4: secure client on a protected computer and network or protected computer, plus a basic form of proctoring

3. As online proctoring takes place in an uncontrolled environment, it is not sufficiently fraud-proof. See a comprehensive analysis in the Online Proctoring white paper. Questions and answers about remote surveillance by SURFnet.
4. There are types of online proctoring available that automatically detect abnormal behaviour and only display camera images to the proctor. At the time of writing, these solutions are still at an early stage of development and are therefore not yet fully reliable. This may nevertheless change in the future.
5. There are assessment environments that use their own environment instead of the operating system on the laptop. This can either be on a USB stick or a server belonging to the institution. This prevents the operating system on the student's computer from loading and makes it more difficult to commit fraud.
6. As part of this solution, a supervisor is still present in the room. Online proctoring therefore serves solely as an additional security measure. Proctoring may involve looking at the candidate's screen instead of camera surveillance.


### Credits

**Author:** Lex Sietses
**Contributions by:** Josephine Verstappen, Willem Brouwer, Jenny de Werk, Michiel van Geloven, Annette Peet
**Photography:** Lars van Rooijen Fotografie, Yuri Samoilov www.flickr.com/photos/yusamoilov/13334048894

**SURFnet**
admin@surfnet.nl www.surf.nl/surfnet



SURF NET