xquiry
educational
data forensics

Educational Data Forensics [EDF] Protocol

an evidence based quality assurance protocol for securing
the process of examination

Amersfoort, August 28, 2018

Inhoudsopgave

The Educational Data Forensics Protocol

The EDF protocol is a quality assurance system, aimed at the prevention (i.e., the prevention of exam fraud as much as possible in advance) and detection (i.e. by means of data forensics after examination) of misconduct in the exam process. Although exam fraud can never be fully banned, the protocol provides standards covering the entire process of examination in order to limit the chances of security risks. That is why the interaction with the EDF monitor is of the utmost importance, because it can highlight fraud trends and possible security gaps. The EDF protocol contains ten standards that together guarantee the security of the exam process.

Scoring

The standards of the protocol show, by means of an assessment of the underlying criteria, at which points the protection of the examination process is good, sufficiently or insufficiently guaranteed.

There are four scoring options for each criterion with the following meaning:
[n.a.] : this criterion does not apply to this exam
[0] insufficient : this criterion is not met
[1] sufficient : this criterion is met
[2] good : The criteria are amply met / demonstrates how this is acted upon

Scores on these standards are then converted to a low security risk or a medium / high security risk. When all criteria are assessed at least with a sufficient level, there is a low risk. When it comes to human actions we can never fully exclude risks, as a result the best possible score for each standard is a low security risk. If one or more criteria per standard are considered insufficient, depending on the impact this part has on the exam, there is a medium or high security risk. Additionally a notes table is included to provide evidence for each standard.

1. Security plan

Criteria	Description	n.a	0	1	2
Security Plan	Security plan; [1]exists as an internal document approved by the management, and [2]is made available to all personnel involved in the process of examination	☐	☐	☐	☐
Security Goals	A mission statement on security goals is present *Goals include at least:* [1]an aim towards preventing disclosure of exam content as much as possible, and [2]a statement of how security is integrated with practice.	☐	☐	☐	☐
Security Policy	Policy governing security efforts provide adequate directions for security measures *Policy includes at least:* [1]Everyone who has access to the content of the exam signed an agreement which prohibits the disclosure of exam content	☐	☐	☐	☐
Actuality	The security plan; [1]is reviewed/revised within the past 12 months, and [2]is discussed internally in the past 12 months	☐	☐	☐	☐
Financial Resources	The security costs; [1]are included in the budget for maintenance and development of the exam. [2]Budget are in accordance with the security plan	☐	☐	☐	☐

Determining security risk for Standard 1	
The total score on this standard is '5' or 'higher', without an 'insufficient' score (a 'not applicable' score lowers the total possible score)	→ Low security risk
Depending on the impact for the exam, one or more 'Insufficient' score(s) on one of the criteria ***Advise***: Direct your resources towards the criteria with the 'Insufficient' score.	→ Medium / High security risk

Available Evidence and Notes for Standard 1	
Security Plan	
Security Goals	
Security Policy	
Actuality	
Financial Resources	

2. Involved personnel: tasks and responsibilities

Criteria	Description	n.a	0	1	2
Security Officer	A chief security officer is appointed. Responsibilities include at least; [1]responsible for discussing integrity and security awareness with all personnel involved in the process of examination, and [2]responsible for compliance with the security plan	☐	☐	☐	☐
Exam Process Members	All personnel involved in the process of examination; [1]sign a confidentiality form, [2]and are authorized by management (personnel include among others, item constructors, proctors, assessors, psychometricians)	☐	☐	☐	☐
Responsibilities	There is a clear division of [1]responsibilities, [2]assignments/tasks and [3]roles for all personnel involved in the process of examination	☐	☐	☐	☐
Competency	Members receive appropriate training in parts of the security plan and associated security policies and procedures that are relevant to their tasks and responsibilities	☐	☐	☐	☐

Determining security risk for Standard 2	
The total score on this standard is '4' or 'higher', without an 'insufficient' score (a 'not applicable' score lowers the total possible score)	→ Low security risk
Depending on the impact for the exam, one or more 'Insufficient' score(s) on one of the criteria ***Advise***: Direct your resources towards the criteria with the 'Insufficient' score.	→ Medium / High security risk

Available Evidence and Notes for Standard 2	
Security Officer	
Exam Process Members	
Responsibilities	
Team Competency	

3. Exam development process and maintenance

Criteria	Description	n.a	0	1	2
Content Development	All activities in the area of exam development take place in a secure (online) environment	☐	☐	☐	☐
Exam Construction	[1]There is a clear distinction between the various stages of exam development (intermediate products, and the final exam). [2]These are not made available for use	☐	☐	☐	☐
Items	[1]The item bank is large enough to offer multiple equivalent exams. The development process is designed in such a way that it is possible to [2]monitor and control possible disclosure of exam content, and [3]in the event of a security incident a replacement process will take effect	☐	☐	☐	☐
Storage	The exam (all exam content) is stored in a secure location	☐	☐	☐	☐

Determining security risk for Standard 3	
The total score on this standard is '4' or 'higher', without an 'insufficient' score (a 'not applicable' score lowers the total possible score)	→ Low security risk
Depending on the impact for the exam, one or more 'Insufficient' score(s) on one of the criteria ***Advise***: Direct your resources towards the criteria with the 'Insufficient' score.	→ Medium / High security risk

Available Evidence and Notes for Standard 3	
Content Development	
Exam Construction	
Items	
Disclosure	
Storage	

4. Security of Examination

Criteria	Description	n.a	0	1	2
Proctoring	[1]Before examination the proctor makes sure control takes place on use of unauthorized materials [2] Proctors observe candidates during examination directly (e.g. cameras or other tools)	☐	☐	☐	☐
Identification	[1]A correct and conclusive identification procedures of examinees prior to examination take place [2]A list is kept with individuals who are excluded from examination	☐	☐	☐	☐
Instruction	[1]The proctor informs examinees of the fact that security measures take place (e.g. data forensics, observations)	☐	☐	☐	☐
Plan and Act	[1]Appropriate security interventions are described, and [2]come into effect if the situation gives reason to do so	☐	☐	☐	☐
Reporting	There is a contact option for examinees or proctors to report suspicious activities before, during or after the examination	☐	☐	☐	☐

Determining security risk for Standard 4	
The total score on this standard is '5' or 'higher', without an 'insufficient' score (a 'not applicable' score lowers the total possible score)	→ Low security risk
Depending on the impact for the exam, one or more 'Insufficient' score(s) on one of the criteria ***Advise***: Direct your resources towards the criteria with the 'Insufficient' score.	→ Medium / High security risk

Available Evidence and Notes for Standard 4	
Proctoring	
Identification	
Instruction	
Plan and Act	
Reporting	

5. Security of Results

Criteria	Description	n.a	0	1	2
Plan	[1]An action plan for screening and investigating deviations and errors in exam results is present, and [2]procedures for subsequent sanctioning if fraud is detected are described	☐	☐	☐	☐
Screening	Screening of the exam results for [1]possible security incidents, and [2]their effect on exam results take place (after every examination)	☐	☐	☐	☐
Transfer	All relevant data (results, reports with deviations and/or suspicious activities) are sent to responsible parties (immediately after examination)	☐	☐	☐	☐
Assessor	[1]Clearly described whether personnel is assigned to assess and/or administer exam results (internal or external). [2]There is a clear division of [1]responsibilities, and [2]tasks for all personnel involved in the process assessing	☐	☐	☐	☐
Sharing Results	Sharing information regarding exam results and candidates takes place according to the established policy and procedures (e.g. appeal procedure)	☐	☐	☐	☐

Determining security risk for Standard 5	
The total score on this standard is '5' or 'higher', without an 'insufficient' score (a 'not applicable' score lowers the total possible score)	→ Low security risk
Depending on the impact for the exam, one or more 'Insufficient' score(s) on one of the criteria ***Advise***: Direct your resources towards the criteria with the 'Insufficient' score.	→ Medium / High security risk

Available Evidence and Notes for Standard 5	
Plan	
Screening	
Transfer	
Assessor	
Sharing Results	

6. Data Forensics: detecting aberrant patterns in test data

Criteria	Description	n.a	0	1	2
Data Forensics	[1]Clearly described whether personnel is assigned to analyse exam results (internal or external). [2]This/these member(s) deliver periodic reports with findings and recommendations	☐	☐	☐	☐
Compromised items	Data forensics include analysing the test items' validity (analysis of: P-value, Differential Item Functioning) Strong aberrant patterns may indicate one or more compromised items	☐	☐	☐	☐
Response Similarity	Data forensics include analysing the test on similarity of responses between candidates Strong aberrant patterns may indicate answer copying or collusion	☐	☐	☐	☐
Response Time	Data forensics include analysing the test on candidates' or item response time Strong aberrant patterns may indicate collusion or harvesting	☐	☐	☐	☐

Determining security risk for Standard 6	
The total score on this standard is '4' or 'higher', without an 'insufficient' score (a 'not applicable' score lowers the total possible score)	→ Low security risk
Depending on the impact for the exam, one or more 'Insufficient' score(s) on one of the criteria ***Advise***: Direct your resources towards the criteria with the 'Insufficient' score.	→ Medium / High security risk

Available Evidence and Notes for Standard 6	
Data Forensics	
Compromised items	
Response Similarity	
Response Time	

7. Security incident response

Criteria	Description	n.a	0	1	2
Incident Response	Clearly defined procedures are in place that include [1]how to report and document security issues, [2]steps for response [3]and follow up	☐	☐	☐	☐
Incident management	[1]There are guidelines and policies in place that are shared all relevant personnel involved in the process of examination, [2]also including a clear description of responsibilities	☐	☐	☐	☐
Sanctioning	In terms of sanctioning; [1]decision-making criteria, [2](legal) procedures and [3]requirements regarding the scope and fairness of the decision-making process have been specified	☐	☐	☐	☐
Sanctioning Responsibility	[1]A person or committee has been appointed and authorized to assess accusations of exam fraud and to impose sanctions, [2]and the disclosure of imposed sanctions is treated confidentially	☐	☐	☐	☐

Determining security risk for Standard 7	
The total score on this standard is '4' or 'higher', without an 'insufficient' score (a 'not applicable' score lowers the total possible score)	→ Low security risk
Depending on the impact for the exam, one or more 'Insufficient' score(s) on one of the criteria ***Advise***: Direct your resources towards the criteria with the 'Insufficient' score.	→ Medium / High security risk

Available Evidence and Notes for Standard 7	
Incident Response	
Incident management	
Sanctioning	
Sanctioning Responsibility	

8. Internet Screening

Criteria	Description	n.a	0	1	2
Monitoring	A formal screening plan ensures regular monitoring (within the last 12 months) of the internet and other media for activities that indicate the possible disclosure of exam components or the sharing of copyright information	☐	☐	☐	☐
Reporting	Ensures the periodic preparation of reports with findings and recommendations based on the screening	☐	☐	☐	☐
Evaluation	Ensures periodic evaluation of the activities in this context (within the last 12 months)	☐	☐	☐	☐
Act	An action plan exists for dealing with alleged or actual theft through the internet of exam content	☐	☐	☐	☐

Determining security risk for Standard 8	
The total score on this standard is '4' or 'higher', without an 'insufficient' score (a 'not applicable' score lowers the total possible score)	→ Low security risk
Depending on the impact for the exam, one or more 'Insufficient' score(s) on one of the criteria ***Advise***: Direct your resources towards the criteria with the 'Insufficient' score.	→ Medium / High security risk

Available Evidence and Notes for Standard 8	
Monitoring	
Reporting	
Evaluation	
Act	

9. Data Forensics: following a suspicion of fraud

Criteria	Description	n.a	0	1	2
Pre-Knowledge (individual)	Following a suspicion of fraud, data forensics include analysis of possible pre-knowledge on an individual level	☐	☐	☐	☐
Pre-Knowledge (group)	Following a suspicion of fraud, data forensics include analysis of possible pre-knowledge on a group level	☐	☐	☐	☐
Collusion	Following a suspicion of fraud, data forensics include analysis of possible collusion	☐	☐	☐	☐
Harvesting	Following a suspicion of fraud, data forensics include analysis of possible harvesting	☐	☐	☐	☐
Answer changing	Following a suspicion of fraud, data forensics include analysis of possible answer changing	☐	☐	☐	☐

Determining security risk for Standard 9	
The total score on this standard is '5' or 'higher', without an 'insufficient' score (a 'not applicable' score lowers the total possible score)	→ Low security risk
Depending on the impact for the exam, one or more 'Insufficient' score(s) on one of the criteria ***Advise***: Direct your resources towards the criteria with the 'Insufficient' score.	→ Medium / High security risk

Available Evidence and Notes for Standard 9	
Pre-Knowledge (individual)	
Pre-Knowledge (group)	
Collusion	
Harvesting	
Answer changing	

10. Performing Security Audit

Criteria	Description	n.a	0	1	2
Responsibility	[1]Responsibility for managing the security audit process is clearly defined, [2]also a standardised procedure ensures the consistent execution of the audit procedures	☐	☐	☐	☐
Archiving	[1]An archive is kept of security audits including the results of these audits	☐	☐	☐	☐
Security Audit	Security audit completed within de last 24 months (based on all EDF protocol security standards or equivalent security standards)	☐	☐	☐	☐
Updating Security Plan	In case of security risks, the security plan is reviewed/revised within 12 months	☐	☐	☐	☐

Determining security risk for Standard 10	
The total score on this standard is '5' or 'higher', without an 'insufficient' score (a 'not applicable' score lowers the total possible score)	→ Low security risk
Depending on the impact for the exam, one or more 'Insufficient' score(s) on one of the criteria ***Advise***: Direct your resources towards the criteria with the 'Insufficient' score.	→ Medium / High security risk

Available Evidence and Notes for Standard 10	
Responsibility	
Archiving	
Security Audit	
Updating Security Plan	