PEER REVIEW NEW PROGRAMME

ADVANCED MASTER IN PRIVACY, CYBERSECURITY, DATA MANAGEMENT AND LEADERSHIP

MAASTRICHT UNIVERSITY

REPORT

22 December 2021

On 27 September 2020 a panel of independent peers including a student has reviewed the quality of the new programme WO-MA Advanced Master in Privacy, Cybersecurity, Data Management and Leadership, Maastricht University (008964). The panel consisted of the following peer experts:

1. Prof. dr. ir. B. (Bart) Preneel, full professor Information Security, KU Leuven (*chair*);
2. Prof. dr. G.P. (Jeanne) Mifsud Bonnici, full professor in European Technology Law and Human Rights, Faculty of Law, University of Groningen;
3. J. (Judith) Rauhofer[1], Senior Lecturer in IT Law at the University of Edinburgh, Associate Director of the Centre for Studies of Intellectual Property and Technology Law (SCRIPT);
4. D. (Diana) van Wanrooij LLM, student in International and European Law, Tilburg University (*student*).

The panel reached a conditionally positive conclusion regarding the quality of the academic master Advanced Master in Privacy, Cybersecurity, Data Management and Leadership offered by Maastricht University. The panel concluded that the programme complies with standards 1 and 3 of the limited NVAO framework and partially complies with standard 2. The panel formulated the following conditions to be met within one year to be fully compliant.

1. The programme has to strengthen the overall alignment between the courses and to make this alignment more explicit for lecturers and students. There is a need for a comprehensive and coherent narrative on the learning outcomes of the courses in relation to the intended learning outcomes of the programme as a whole and the envisioned graduate.
2. The programme needs to provide a course to help applicants with non-legal backgrounds pass the entrance exam on EU law.

For further improvement to the programme, the panel recommended several follow-up actions.

1. Intake process – Make sure that the weight of admission criteria is in line with the programme's target group, by putting more emphasis on work experience and less on bachelor grades.

2. Balance between academic and practical skills – The practical approach of the programme is a strong point, but ensure that this does not detract from the development of critical thinking and analytic skills which should form part of the research component.

3. Continuity – Be aware that contributions from other university departments and external experts may be compromised by changing priorities on their side and anticipate on this by clarifying agreements and commitments.

4. Quality of assessment – Ensure that the validity and transparency of exams and assignments is checked by an independent referent before the examination. Ensure full interdisciplinarity in the supervision and assessment of interdisciplinary thesis projects, including where this would require the provision of more than one supervisor.

On 4 May 2021, the University of Maastricht sent detailed information that indicated how the programme was adjusted in order to meet the conditions, including a full update of the Course Manual. On 18 August 2021, the panel has requested some clarifications from the University of Maastricht. On 15 September 2021, the University of Maastricht has provided an answer to the questions.

This report contains the findings, analysis and judgements of the panel resulting from the peer review.

[1] Currently at Digital Freedom Fund

Summary

The panel appreciates the excellent quality of the documentation provided by the programme, with clear indications to what has been changed with respect to the previous version. After careful analysis of the documentation and the answer to the additional questions, the panel concludes that the two conditions imposed by the peer review report have been satisfied.

Evaluation of the Conditions

Condition 1: *The programme has to strengthen the overall alignment between the courses and to make this alignment more explicit for lecturers and students. There is a need for a comprehensive and coherent narrative on the learning outcomes of the courses in relation to the intended learning outcomes of the programme as a whole and the envisioned graduate.*

The panel concludes that the intended learning outcomes have been revised and a detailed mapping has been provided of the course intended learning outcomes to the programme intended learning outcomes. In addition, clear learning lines have been created and they are carefully explained. In every course description, the relationship between courses is being provided. Any overlap that existed between the courses has been removed Overall, a clear and coherent narrative is now present on the intended learning outcomes.

Condition 2: *The programme needs to provide a course to help applicants with non-legal backgrounds pass the entrance exam on EU law.*

A prerequisite course on "Introduction to European Union Law" has been added. The content and approach of this course is fully appropriate for the intended goals.

Title change

The programme proposes to change the title of the programme to Advanced Master in Privacy, Cybersecurity and Data Management. The panel agrees with this minor change.

Follow-up Actions

This section comments on the progress with respect to the follow-up actions suggested in the peer review report.

1. Intake process – Make sure that the weight of admission criteria is in line with the programme's target group, by putting more emphasis on work experience and less on bachelor grades.

The panel notes that the revised procedure addresses this comment in full: priorities have been assigned to the admission criteria and the position of junior applicants has been clarified.

2. Balance between academic and practical skills – The practical approach of the programme is a strong point, but ensure that this does not detract from the development of critical thinking and analytic skills which should form part of the research component.

The panel concludes that this balance is taken into account in all the courses and notes that this balance will form an important guiding element for the master thesis.

3. Continuity – Be aware that contributions from other university departments and external experts may be compromised by changing priorities on their side and anticipate on this by clarifying agreements and commitments.

This panel is satisfied that the risks related to external teachers are carefully managed. In addition, the panel notes that appropriate agreements are in place for ensuring coherent cooperation with the Department of Data Science and Knowledge Engineering (DKE) - Faculty of Science and Engineering- for the delivery of the orientation course "Introduction to Computer Science and New Technologies" and with the UMIO - Maastricht University School of Business and Economics (SBE) for the delivery of the course "Leadership Development Trajectory".

4. Quality of assessment – Ensure that the validity and transparency of exams and assignments is checked by an independent referent before the examination. Ensure full interdisciplinarity in the supervision and assessment of interdisciplinary thesis projects, including where this would require the provision of more than one supervisor.

The panel concludes that there is a clear plan to ensure that the validity and transparency of exams and assignments and that the four-eye principle is applied. From the information provided, the panel deduces that quality checks by an independent expert may happen after rather than before the examination. The panel is satisfied with the modifications of the regulations for the evaluation of the Master's Thesis: inter-disciplinary theses can be accommodated through the appointment of two supervisors and a third assessor.

Overall, the panel concludes that the follow-up actions in the peer review report have been addressed in a satisfactory way.

Additional Feedback

The panel offers some comments and suggestions with respect to specific courses:

1. Course Introduction to Computer Science and New Technologies:

- It should be clarified whether the item "software and virtual machines" also includes cloud technologies.

2. Course EU and Global Cybersecurity Fundamentals:

- It should be considered to add the EU Cybersecurity Act to the course literature.
- The course description mentions threats and network security and describes the general approach taken by the book by Stallings and Brown. It mentions a few topics from Part 1 of this book (e.g., access control); the section on building blocks lists Chapters 6-9. Perhaps the course description could explain more clearly what will be covered and what will not be covered: 1) cryptography is covered in the advanced course; 2) network security is mentioned where probably computer security or cybersecurity is intended.

3. Course Advanced Cybersecurity and Global Cybersecurity Strategy:

- The relationship with the course EU and Global Cybersecurity Fundamentals could be explained better.
- This course description mentions some items that should perhaps be covered under fundamentals such as “key information security principles” and “threats, attacks, exploits and vulnerabilities”. Note that some of the technical concepts seem to be required for the course Comprehensive Risk Assessment and DPIA.

The panel offers some comments and suggestions with respect to specific topics:

1. The programme should consider giving more attention to legal aspect of cybercrime.

2. It is not sufficiently clear where in the programme the economic and psychological aspects of cybersecurity are covered. Some references are offered that are relevant for these topics.

- https://www.cl.cam.ac.uk/~rja14/econsec.html
- M. Felici, N. Wainwright, S. Cavallini, F. Bisogni, "What's New in the Economics of Cybersecurity?," in IEEE Security & Privacy, vol. 14, no. 03, pp. 11-13, 2016 https://doi.ieeecomputersociety.org/10.1109/MSP.2016.64
- B. Schneier, “The psychology of security,” Communications of the ACM 50(5): 128 (2007)
- R.A.M. Lahcen, B.D. Caulkins, R.N. Mohapatra, M. Kumar, “Review and insight on the behavioral aspects of cybersecurity,” Cybersecurity 3(1): 10 (2020) https://doi.org/10.1186/s42400-020-00050-w