TECHNISCHE HOCHSCHULE DEGGENDORF

Akkreditierungsurkunde

Der Studiengang

Cyber Security

Master of Engineering (M.Eng.)

hat das interne Verfahren zur Qualitätssicherung mit Erfolg durchlaufen. Die Akkreditierung erfolgte durch ein Internes Audit, welches mit der Verleihung des Siegels des Akkreditierungsrates abschließt.

Die Technische Hochschule Deggendorf ist seit dem 09.09.2020 durch die Akkreditierungsagentur ASIIN systemakkreditiert und damit berechtigt, die Qualität ihrer Studiengänge anhand der European Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG), des Qualifikationsrahmens für deutsche Hochschulabschlüsse und den Vorgaben aus dem Studienakkreditierungsstaatsvertrag in Verbindung mit der Bayerischen Studienakkreditierungsverordnung (BayStudAkkV) selbst zu prüfen und zu akkreditieren.

Der Beschluss über die Akkreditierung erfolgt auf Basis der Ergebnisse des Internen Audits und der vorgeschlagenen Auflagen und Empfehlungen durch das Auditierungsgremium.

Die Akkreditierung wurde am 08.06.2020 vom internen Akkreditierungsgremium unter Auflagen beschlossen und ist bis zum 28.04.2026 befristet. Auflagen wurden fristgerecht erfüllt.

SYSTEM AKKREDITIERT
Akkreditierungsrat

Deggendorf, 26.04.2021

Prof. Dr. Peter Sperber
Präsident

Kurzbeschreibung des Verfahrens

Die internen Akkreditierungen (= Interne Audits) finden alle sechs Jahre statt. Die Gutachtergruppen setzen sich aus jeweils mindestens vier Personen aus verschiedenen Bereichen zusammen, was eine umfassende Einschätzung der Qualität eines Studiengangs sicherstellt:

- Mindestens zwei Professor:innen von Hochschulen und Universitäten (ein:e Vertreter:in extern, ein:e Vertreter:in intern)
- Mindestens ein:e Vertreter:in der Berufspraxis, Industrie- oder Unternehmensvertreter:in
- Mindestens ein:e Vertreter:in der Studierenden, welche:r im Moment den gleichen bzw. einen ähnlichen Studiengang an einer anderen Hochschule bzw. Universität studiert oder vor kurzem abgeschlossen hat.

Die Begutachtung der formalen Akkreditierungsanforderungen und hochschulrechtlichen Vorgaben erfolgt bereits vorab im Rahmen der formellen Prüfung des Studiengangs durch das ZQM, wird aber mit den Gutachter:innen nochmal aufgegriffen.

Die Überprüfung der für den jeweiligen Studiengang erforderlichen personellen und sächlich-räumlichen Ressourcen erfolgt durch die zuständige Fakultät, wird aber am Audittag auch nochmal aufgegriffen, um den Gesamteindruck des Studiengangs zu bewerten. Darüber hinaus bewerten die Verantwortlichen der Fakultät sowohl die fachlich-inhaltlichen als auch die formellen Kriterien innerhalb eines Selbstaudits und füllen eine Fakultätscheckliste aus.

Der Audittag ist so gestaltet, dass vom ZQM gezielt auf die Fragen und Bemerkungen eingegangen wird, welche die Gutachter:innen im Vorfeld bei einer Online-Befragung mit EvaSys beschrieben haben. Hierzu wurde den Gutachter:innen eine Checkliste zur Verfügung gestellt, die die relevanten Punkte der BayStudAkkV abdeckt. Im Fokus steht eine fachlich-inhaltliche Bewertung des Studiengangs und des zugrunde gelegten Konzepts anhand der Gesamtdokumentation, die per Cloud geteilt wird.

Damit eine ganzheitliche Bewertung des Studiengangs möglich ist, sind bei einem Internen Audit Befragungen von Lehrenden und Studierenden des Studiengangs vorgesehen.

Die Internen Audits dienen zur Überprüfung, ob diese Prozesse auf der Ebene des Studiengangs umgesetzt und „gelebt" werden. Die Verfahren weisen einen hohen Beratungscharakter auf und sind von einer großen Offenheit und gegenseitigem Respekt geprägt.

Zwischen zwei Audits, also nach drei Jahren, wird eine kleine Überprüfung des Studiengangs (= Internes Review) vorgenommen, um festzustellen, ob das Studiengangskonzept inkl. Qualifikationsprofil noch aktuell ist oder ob Verbesserungsbedarf besteht. Auch bei einem Internen Review wird der Studiengang gemeinsam mit Industrievertreter:innen / Vertreter:innen der Berufspraxis, Studierenden / Absolvent:innen und Lehrenden auf Aktualität und Adäquanz der Inhalte überprüft und ein Protokoll über mögliche Maßnahmen erstellt. Eine Umsetzung wird beim nächsten Internen Audit überprüft.

Kurzprofil des Studiengangs

Hochschule	Technische Hochschule Deggendorf			
Ggf. Standort	Campus Deggendorf			
Studiengang (Name/Bezeichnung) ggf. inkl. Namensänderungen	Cyber Security			
Abschlussgrad / Abschlussbezeichnung	Master of Engineering (M.Eng.)			
Studienform	Präsenz	☒	Blended Learning	☐
	Vollzeit	☐	Intensiv	☐
	Teilzeit	☒	Joint Degree	☐
	Dual	☐	Lehramt	☐
	Berufsbegleitend	☒	Kombination	☐
	Fernstudium	☐	Double Degree	☐
Regelstudienzeit (in Semestern)	5			
Zulassungsvoraussetzungen	Abgeschlossenes Erststudium aus dem Bereich der Ingenieurswissenschaften oder Informatik an einer anerkannten Hochschule, mindestens 1 Jahr Berufserfahrung nach Abschluss des Erststudiums, erfolgreiches Durchlaufen des Bewerbungsverfahrens inkl. eines Orientierungsgesprächs mit dem Studiengangsleiter			
Anzahl der vergebenen ECTS-Punkte	90			
Bei Master: konsekutiv oder weiterbildend	konsekutiv			
Unterrichtssprache	Deutsch			
Kooperationen (studiengangsbezogen)	-			
Studienbeginn	Jährlich zum Sommersemester			
Anzahl Studienanfänger pro Semester	Max. 15 Anfänger			
Studiengangskoordinator	Prof. Dr. Andreas Grzemba.			

Die Studierenden besitzen nach Abschluss des berufsbegleitenden Masterstudienganges Cyber Security die Fähigkeit, Bedrohungen und Gefahren für individuelle Anwendungsfälle zu erkennen und zu formulieren, das resultierende Risiko zu analysieren sowie selbstständig geeignete Sicherheitsstrategien zu erarbeiten und umzusetzen. Weiter sind die Studierenden durch das vermittelte Wissen des berufsbegleitenden Masterstudienganges Cyber Security in der Lage, Sicherheitsvorfälle in den Bereichen Industrial und Automotive zu erkennen und darzustellen, was sowohl bei forensischen Untersuchungen als auch beim Informationssicherheitsmanagement unerlässlich ist. Durch heterogene Studiengruppen werden die Studierenden auf ihr späteres Arbeitsleben im Unternehmen vorbereitet. In den Semestern zwei und vier vertiefen die Studierenden ihr Fachwissen in den Bereichen Industrial und Automotive IT Security. Im Besonderen werden den Teilnehmerinnen und Teilnehmern auch fachübergreifende und internationale Kenntnisse nähergebracht, die sie in die Lage versetzen, Gesamtsysteme und –prozesse zu überschauen. Durch diesen ganzheitlichen Ansatz können Absolventen Probleme nicht nur aus einer fachspezifischen Sicht beurteilen, sondern können den Gesamtnutzen für das Unternehmen optimieren.

Gutachtergruppe beim Internen Audit Master „Cyber Security" am 28.04.2020:

- Prof. Dr. Eckehard Hermann (Fachhochschule Oberösterreich, Campus Hagenberg: Professor für Sichere Softwaresysteme)
- Prof. Dr. Götz Winterfeldt (THD: Fakultät Elektrotechnik und Medientechnik)
- Peter König (Abteilungsleiter Projekte/Systeme, Rohde & Schwarz GmbH & Co. KG, Werk Teisnach, Vertreter der Berufspraxis)
- Florian Hehenberger (Absolvent des Bachelors „Sichere Informationssysteme", aktuell Student im Master „Sichere Informationssysteme an der Fachhochschule Oberösterreich, Campus Hagenberg)

Beschlussempfehlung der Gutachter:innen:

Auf Basis der eingereichten, studiengangsspezifischen Unterlagen und der Dokumentation des Internen Audits haben die Gutachter:innen festgestellt:

	Ja	Nein
Die formalen Kriterien sind erfüllt.	☐	☒
Die fachlich-inhaltlichen Kriterien sind erfüllt.	☒	☐

Auflagen und Empfehlungen des Gutachterteams zur Weiterentwicklung des Studiengangs Master „Cyber Security":

Auflagen: von den Gutachtern wurden keine Auflagen ausgesprochen.

Empfehlungen:

Empfehlung zu Formale Kriterien Modularisierung Punkt 1: *Sind alle Module des Studiengangs im Modulhandbuch der Fakultät beschrieben und enthalten die vorgegeben Inhalte als Mindestanforderung?*

- Überarbeitung des Modulhandbuchs an den genannten Stellen notwendig.
  CY-06: Keine Workload und Lehrform angegeben. CY-10: Lehrform, Verwendbarkeit, Voraussetzungen für die Vergabe von Leistungspunkten nicht angegeben CY-I07: Keine Gewichtung der Note angegeben;

Teilweise ist die Referenzliteratur recht alt und auch in unterschiedlichen Auflagen (z.B. Buch von C. Eckert). Literatur zu Schwerpunkten fehlt (z.B. zum Thema Secure Software Eng. In Security Engineering 1).

Empfehlung zu Formale Kriterien Modularisierung Punkt 5: *Ist eine ausreichende Prüfungsvielfalt vorgesehen? Passen die Prüfungen zu den jeweiligen Fachinhalten?*

- Überprüfung der StPrO notwendig. Es soll überprüft werden, ob z.T. mündliche Prüfungen oder Studienarbeiten in das Curriculum integriert werden können. Z.B. bei Modul 4 könnte eine Studienarbeit als Prüfungsform eingesetzt werden.

Empfehlung zu Formale Kriterien Anerkennung Punkt 1: *Sind die Regelungen zur Anerkennung definiert oder wird in der Studien- und Prüfungsordnung darauf hingewiesen?*

- In der StPrO sollte auf die Anerkennungsrichtlinie hingewiesen werden.

Empfehlung zu Formale Kriterien Studien- und Prüfungsordnung Punkt 1: *Sind Umfang und Dauer der Vorlesungen im Anhang der PO aufgelistet (SWS, ECTS)?*

- In der StPrO sollten die Prüfungs- bzw. Unterrichtssprachen definiert werden (Deutsch/Englisch).

Beschluss des internen Akkreditierungsgremiums an der Technischen Hochschule Deggendorf vom 08.06.2020:

Das Akkreditierungsgremium hat am 08.06.2020 beschlossen, den Studiengang Master „Cyber Security" mit den Empfehlungen der Gutachter:innen zu akkreditieren.
Die Empfehlung zu Formale Kriterien Modularisierung Punkt 1: *Sind alle Module des Studiengangs im Modulhandbuch der Fakultät beschrieben und enthalten die vorgegeben Inhalte als Mindestanforderung* wurde vom Akkreditierungsgremium **zu einer Auflage hochgestuft**, da die aufgeführten Mängel schnellstmöglich korrigiert werden müssen.

- Überarbeitung des Modulhandbuchs an den genannten Stellen notwendig.
  CY-06: Keine Workload und Lehrform angegeben. CY-10: Lehrform, Verwendbarkeit, Voraussetzungen für die Vergabe von Leistungspunkten nicht angegeben CY-I07: Keine Gewichtung der Note angegeben;
  Teilweise ist die Referenzliteratur recht alt und auch in unterschiedlichen Auflagen (z.B. Buch von C. Eckert). Literatur zu Schwerpunkten fehlt (z.B. zum Thema Secure Software Eng. In Security Engineering 1).

Die Empfehlung zu Formale Kriterien Studien- und Prüfungsordnung Punkt 1: *Sind Umfang und Dauer der Vorlesungen im Anhang der PO aufgelistet (SWS, ECTS)* **wurde zu einer Anmerkung herabgestuft**, da dies auch über den Studienplan erfolgen kann.

- In der StPrO sollten die Prüfungs- bzw. Unterrichtssprachen definiert werden (Deutsch/Englisch).

Der Studiengang wurde im Verfahren anhand der Mindestanforderungen geprüft.

Ergebnis:

	Ja	Nein
Die formalen Kriterien sind erfüllt.	☐	☒
Die fachlich-inhaltlichen Kriterien sind erfüllt.	☒	☐

Das Akkreditierungsgremium spricht für den Masterstudiengang „Cyber Security" (M.Eng.) eine Verleihung des Siegels des Akkreditierungsrates bis zum 28.04.2026 mit einer Auflage und zwei Empfehlungen aus.

Auflagenerfüllung

Überprüfung der Auflagenerfüllung durch das ZQM:
Zunächst ist anzumerken, dass sich das Modulhandbuch im Moment noch in Überarbeitung befindet, da die beiden Schwerpunkte (Industrial IT Security und Automotive IT Security) im Rahmen des neuen Studiengangskonzepts nicht mehr vorgesehen sind. Dieser Wegfall der inhaltlichen Schwerpunkte wurde mit dem Zentralen Qualitätsmanagement abgesprochen und ist somit von der geltenden Akkreditierung umfasst.

Im Rahmen der Überarbeitung des Modulhandbuchs wurde im Modul CY-06 die Workload und die Lehrform ergänzt. Das Modul CY-I07 existiert in der aktuellen Studien- und Prüfungsordnung nicht mehr, dieses wurde mit CY-A07 zusammengelegt. Im aktuellen Modul zu CY-07 wurde die Gewichtung der Note ergänzt. In der ausgesprochenen Auflage haben die Gutachter zudem darauf hingewiesen, dass die Referenzliteratur, die angegeben wurde, fehlte oder veraltet war. Die Referenzliteratur z.B. zu Security Engineering wurde umfangreich überarbeitet und um aktuelle Literatur ergänzt. Das ZQM bewertet die Auflage an dieser Stelle als erfüllt, das aktuelle Modulhandbuch wird in der Nextcloud für das Akkreditierungsgremium hinterlegt.

Zum 15.03.2021 trat die neue Studien- und Prüfungsordnung des Masters Cyber Security in Kraft. In dieser wurde die Empfehlung der Gutachter berücksichtigt und es wurden mehr mündliche Prüfungen eingeführt. So wird z.B. M-CY-09 nun auch anhand einer mündlichen Prüfung abgeprüft. Das ZQM möchte an dieser Stelle jedoch darauf hinweisen, dass die Dauer der mündlichen und schriftlichen Prüfungen leider nicht in der Studien- und Prüfungsordnung festgelegt ist, das muss nachgeholt werden. Die Empfehlung der Gutachter wurde jedoch berücksichtigt und wird als erfüllt angesehen.

Darüber hinaus wurde am Audittag die Empfehlung ausgesprochen, in der Studien- und Prüfungsordnung auf die Anerkennungsrichtlinie hinzuweisen. Mit der Referentin für Studien- und Studierendenangelegenheiten wurde mittlerweile geklärt, dass es sich hier um keine Richtlinie, sondern um einen Leitfaden zur Anerkennung handelt. Da dies kein rechtlich bindendes Dokument darstellt, kann in der Studien- und Prüfungsordnung nicht darauf verwiesen werden, die Empfehlung entfällt daher.

Das ZQM bewertet die Auflagen und Empfehlungen, die die Gutachter beim Internen Audit ausgesprochen haben, als erfüllt und befürwortet die Ausweitung des Akkreditierungszeitraums auf die volle Dauer von insgesamt sechs Jahren.

Das interne Akkreditierungsgremium an der Technischen Hochschule Deggendorf stimmt dem ZQM bei der Bewertung der Auflagenerfüllung zu und fasst am 26.04.2021 folgenden Beschluss: Die Auflagen wurden fristgerecht erfüllt.