22/26

9. Juli 2026

Amtliches Mitteilungsblatt

Seite

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

Herausgeber

Das Präsidium der HTW Berlin

Treskowallee 8

10318 Berlin

Redaktion

Justiziariat

Tel. +49 30 5019-2813

Fax +49 30 5019-2815

HOCHSCHULE FÜR TECHNIK UND WIRTSCHAFT BERLIN

Studien- und Prüfungsordnung für den englischsprachigen Bachelorstudiengang

Cyber Security and Business (CSB)

Bachelor of Science (B.Sc.)

im Fachbereich Informatik, Kommunikation und Wirtschaft

vom 15. April 2026

Auf Grund von § 16 Abs. 1 Satz 1 Nr. 1 der Satzung der Hochschule für Technik und Wirtschaft Berlin vom 16. Dezember 2024 (AMBl. HTW Berlin Nr. 12/25) in Verbindung mit § 31 des Gesetzes über die Hochschulen im Land Berlin (Berliner Hochschulgesetz - BerlHG) in der Fassung der Bekanntmachung vom 26. Juli 2011 (GVBl. S. 378), zuletzt geändert durch Gesetz vom 21. Januar 2026 (GVBl. S. 23), hat der Fachbereichsrat des Fachbereiches Informatik, Kommunikation und Wirtschaft der HTW Berlin am 15. April 2026 die folgende Studien- und Prüfungsordnung für den Bachelorstudiengang Cyber Security and Business beschlossen[1]:

Gliederung der Ordnung

[1] Bestätigt durch das Präsidium der Hochschule für Technik und Wirtschaft Berlin am 13. Mai 2026.

§ 1 Geltungsbereich

(1) Diese Studien- und Prüfungsordnung gilt für alle Studierenden, die nach Inkrafttreten dieser Ordnung am Fachbereich Informatik, Kommunikation und Wirtschaft der HTW Berlin im englischsprachigen Bachelorstudiengang Cyber Security and Business in das 1. Fachsemester immatrikuliert werden.

(2) Ferner gilt diese Studien- und Prüfungsordnung für alle Studierenden, die nach einem Hochschul- oder Studiengangwechsel aufgrund der Anrechnung von Studien- und Prüfungsleistungen zeitlich so in den Studienverlauf eingeordnet werden, dass ihr Studienstand dem Personenkreis gemäß Absatz 1 entspricht.

(3) Die Studien- und Prüfungsordnung wird ergänzt durch die Zugangs- und Zulassungsordnung für den englischsprachigen Bachelorstudiengang Cyber Security and Business in der jeweils gültigen Fassung.

§ 2 Geltung von Rahmenordnungen

Die Hochschulordnung (HO) in ihrer jeweils gültigen Fassung, die Grundsätze für Studien- und Prüfungsordnungen für Bachelor- und Masterstudiengänge der Hochschule für Technik und Wirtschaft Berlin (Rahmenstudien- und -prüfungsordnung für Bachelor- und Masterstudiengänge – RStPO – Ba/Ma) in ihrer jeweils gültigen Fassung und die Ordnung für die Durchführung des Fachpraktikums in den Bachelor- und Masterstudiengängen der HTW Berlin (Praxisordnung – PraxO) in ihrer jeweils gültigen Fassung sind Bestandteil dieser Ordnung.

§ 3 Vergabe von Studienplätzen

Die Vergabe von Studienplätzen richtet sich nach dem Berliner Hochschulgesetz, dem Berliner Hochschulzulassungsgesetz und der Berliner Hochschulzulassungsverordnung in ihren jeweils gültigen Fassungen in Verbindung mit der Hochschulordnung und der Auswahlordnung für Bachelorstudiengänge in der jeweils gültigen Fassung, sowie der Zugangs- und Zulassungsordnung für den englischsprachigen Bachelorstudiengang Cyber Security and Business in der jeweils gültigen Fassung.

§ 4 Fachgebundene Hochschulzugangsberechtigung

(1) Für Bewerbungen auf der Grundlage von § 11 Abs. 2 BerlHG werden für den Bachelorstudiengang Cyber Security and Business insbesondere die in Anlage 1 aufgeführten abgeschlossenen Berufsausbildungen als geeignet angesehen.

(2) Über die inhaltliche Vergleichbarkeit von anderen als den in Anlage 1 aufgeführten Berufsausbildungen entscheidet der Prüfungsausschuss des Studienganges.

§ 5 Qualifikationsziele

(1) Ziel des Bachelorstudiums ist es, Absolvent*innen mit dem akademischen Grad Bachelor of Science auszubilden, die in der Lage sind, komplexe Informatikanwendungen für Informationssicherheit zu konzipieren, umzusetzen und weiterzuentwickeln. Hierzu werden in den Pflichtmodulen grundlegende Prinzipien, Methoden, Modelle und Werkzeuge vermittelt, welche die Studierenden zur ganzheitlichen, integrativen Analyse und Realisierung von sicherheitsorientierten Informations- und Kommunikationssystemen in Bezug auf Hard- und Software befähigen. Zusätzlich werden die Studierenden sensibilisiert, auch den Faktor „Mensch" in diesem Kontext einzuordnen. Durch die Integration relevanter Grundlagen der Informatik, der Informationssicherheit sowie der Betriebswirtschaftslehre sollen im Vertiefungsjahr die zur Konzipierung, Entwicklung, Einführung, Nutzung und Wartung sowie zum Verwalten von informationsverarbeiten Systemen notwendigen Kenntnisse und Denkweisen erarbeitet werden. Sie verfügen über fundierte Kenntnisse der Informationssicherheit sowie der IT-Forensik. Mit diesem Wissen arbeiten sie präventiv bei der Absicherung der bestehenden Systeme. Daneben detektieren sie Angriffe oder übernehmen die Verantwortung für die Untersuchungen von Sicherheitsvorfällen.

(2) Lehre und Studium im Bachelorstudiengang Cyber Security and Business an der HTW Berlin sollen die Studierenden auf berufliche Tätigkeiten unter Berücksichtigung von Veränderungen in der Berufswelt und des gesellschaftlichen Umfelds vorbereiten; dies schließt ergänzend zur IT-Sicherheit auch wirtschaftliche, soziale und ethische Aspekte mit ein. Die dafür erforderlichen Kenntnisse, Fähigkeiten und Methoden sollen den Studierenden so vermittelt werden, dass sie zu selbständiger wissenschaftlicher Arbeit, insbesondere zur Anwendung wissenschaftlicher Methoden und Erkenntnisse im Beruf und zu kritischem Denken und verantwortlichem Handeln in der Gesellschaft befähigt werden.

(3) Ein zentrales Ziel des Studiengangs ist die Befähigung der Studierenden zum Agieren in internationalen Kontexten. Daher ist das Studium inhaltlich geprägt durch Fachmodule internationalen Inhalts wie zum Beispiel Digitale Ökonomie, Cloud IT und Mobile Devices sowie eine Fremdsprachenausbildung. Studierende werden befähigt, ökologische, ökonomische und soziale Auswirkungen ihres Handelns kritisch zu reflektieren und verantwortungsvolle Entscheidungen zu treffen. Insbesondere im Kontext der Informationstechnologie und Cyber Security sind die zu erwerbenden Kenntnisse von Nachhaltigkeit bedeutsam, da digitale Systeme, Infrastrukturen und datengetriebene Anwendungen maßgeblich zu Ressourcennutzung, Energieverbrauch und gesellschaftlichem Wandel beitragen. Zusätzlich werden die Besonderheiten der IT-Sicherheit im internationalen Kontext (Internationalisierung von Software, internationale Standards, globale Medien und Netze, etc.) behandelt.

(4) Damit zielt das Studium insgesamt auf eine fachliche und persönliche Befähigung der Absolvent*innen für den Einsatz vorrangig in den Bereichen

- Wirtschafts- und IT-Sicherheit (im Sinne von Security und Safety)
- Wirtschafts- und IT-Sicherheit für kommunale Einrichtungen (Administration)
- Wirtschafts- und IT-Sicherheit und Forensik
- Wirtschafts- und IT-Sicherheit und Distributed-Ledger-Technologie.

§ 6 Regelstudienzeit, Studienplan, Module

(1) Der Bachelorstudiengang Cyber Security and Business wird in englischer Sprache angeboten.

(2) Das Bachelorstudium ist ein Präsenzstudium und hat eine Dauer von sechs Semestern (Regelstudienzeit). Das Bachelorstudium umfasst 180 ECTS-Leistungspunkte. Ein ECTS-Leistungspunkt steht für einen studentischen Arbeitsaufwand von 30 Stunden. Die jährliche Workload für den Bachelorstudiengang Cyber Security and Business beträgt 1800 Stunden.

(3) Das Studium wird im Einzelnen nach dem Studienplan in Anlage 2 durchgeführt und ist gemäß § 4 RStPO - Ba/Ma modularisiert. Er enthält eine Liste aller Module des Bachelorstudiengangs Cyber Security and Business. Er nennt für jedes Modul die Modulbezeichnung, die Niveaustufe, die Form und Art des Modulangebots (Pflicht-/Wahlpflichtmodul), die Präsenzzeit der Lehrveranstaltungen (in SWS), die zugrundeliegende Lernzeit in zu vergebenden ECTS-Leistungspunkten und die notwendigen und empfohlenen Voraussetzungen. Die Wahlpflichtmodule sind in der Anlage 3, die Angebote für AWE-Module/Fremdsprachen in der Anlage 4 aufgeführt.

(4) Für jedes Modul werden ferner Lernergebnisse und Kompetenzen festgelegt, die in Anlage 6 enthalten und Bestandteil dieser Ordnung sind.

(5) Die ausführliche Beschreibung der Module erfolgt in den Modulbeschreibungen für den Bachelorstudiengang Cyber Security and Business.

§ 7 Ablauf des Studiums

(1) Studienbeginn im Bachelorstudiengang Cyber Security and Business ist einmal jährlich jeweils zum Wintersemester.

(2) Das vierte Semester ist als Mobilitätssemester für das Studium an einer anderen Hochschule im In- oder Ausland vorgesehen.

(3) Anstelle eines curricular vorgesehenen Wahlpflichtmoduls (B22, B23, B29 oder B30) im Umfang von fünf ECTS-Leistungspunkten ist es nach Maßgabe freier Plätze gestattet, ein (in englischer Sprache angebotenes) interdisziplinäres Projekt eines der Fachbereiche der HTW Berlin zu absolvieren.

(4) Im 4. und 5. Semester werden Wahlpflichtmodule angeboten. Eine Übersicht der Wahlpflichtmodule mit der Zuordnung zu den Vertiefungen findet sich in Anlage 3.

Aus dem Angebot an Wahlpflichtmodulen müssen Module im Umfang von 20 ECTS-LP absolviert werden. Werden Module im Umfang von 15 ECTS-LP aus einer Vertiefungsrichtung absolviert, wird diese Vertiefung auf dem Bachelorzeugnis ausgewiesen. Ansonsten werden die Module unter fachspezifische Wahlpflichtmodule auf dem Bachelorzeugnis ausgewiesen.

Der oder die Studiengangssprecher*in entscheidet rechtzeitig darüber, welche Module angeboten werden. Auf Grund aktueller Entwicklungen kann der Fachbereichsrat weitere Wahlpflichtmodule beschließen.

(5) In jedem Semester kann ein Modul (im Umfang von fünf ECTS-LP) als E-Learning-Modul angeboten werden. Welches Modul auf diese Art angeboten wird, beschließt der Fachbereichsrat jeweils rechtzeitig vor Semesterbeginn. Als E-Learning-Module können alle Module bis auf das AWE-Modul und Erste Fremdsprache durchgeführt werden.

(6) Das Studium ist erfolgreich abgeschlossen, wenn alle Module sowie die Bachelorarbeit und das Kolloquium jeweils erfolgreich absolviert wurden.

§ 8 Studium Generale

Im Rahmen des Studium Generale stehen Modulangebote zur Verfügung, die der Vermittlung fremdsprachlicher, überfachlicher oder fachübergreifender Kompetenzen im Sinne von § 2 der RStPO – Ba/Ma in der jeweils gültigen Fassung dienen.

§ 9 Studium Generale: Verpflichtende Fremdsprachenausbildung

(1) Im Bachelorstudium ist eine verpflichtende Ausbildung in einer Fremdsprache im Umfang von fünf ECTS-Leistungspunkten vorgesehen. Die Fremdsprachenausbildung dient der Vertiefung bereits vorhandener Kenntnisse in einer Fremdsprache.

(2) Die Studierenden wählen als erste Fremdsprache Englisch oder Französisch oder Spanisch. Der Umfang beträgt fünf ECTS-LP und vier SWS. Die fachsprachliche Ausbildung in der Fachsprache Wirtschaft für die erste gewählte Fremdsprache beginnt in Englisch mindestens auf dem Niveau C1.1. und/oder C1.2. GER, in den anderen Fremdsprachen mindestens auf dem Niveau B1.2 GER.

(3) Studierende, die ihre Hochschulzugangsberechtigung in einer anderen Sprache als Deutsch erworben haben, dürfen im Rahmen der vorgesehenen Fremdsprachenausbildung Deutsch als Fremdsprache (mindestens auf dem Niveau der sprachlichen Anforderungen für den Hochschulzugang) wählen.

(4) Die Sprache der Hochschulzugangsberechtigung des oder der Studierenden ist von der Wahl ausgeschlossen.

§ 10 Studium Generale: Allgemeinwissenschaftliches Ergänzungsmodul (AWE)

Der Umfang des allgemeinwissenschaftlichen Ergänzungsmoduls (AWE-Modul) beträgt fünf ECTS-Leistungspunkte[1]. Das AWE-Modul kann aus dem deutsch- und englischsprachigen AWE-Angebot der HTW Berlin frei gewählt werden. Es gelten im Übrigen die Regelungen gemäß § 10 der RStPO – Ba/Ma in der jeweils gültigen Fassung. Die möglichen Varianten sind in der Anlage 4 dargestellt.

[1] Es können auch zwei Teilmodule zu je zweieinhalb Leistungspunkten absolviert werden.

§ 11 Fachpraktikum

(1) Der Bachelorstudiengang umfasst neben den im Studienplan gemäß Anlage 2 genannten Lehrgebieten ein Fachpraktikum von 15 ECTS-Leistungspunkten, welches in der Regel mit der 24. Woche des 5. Studienplansemester beginnen soll. Sein Umfang entspricht 12 Wochen und ist als Vollzeitpraktikum durchzuführen.

(2) Die Zulassung zum Praktikum muss rechtzeitig vor Beginn des Praktikums bei dem oder der Praxisbeauftragten des Studiengangs beantragt und von diesem oder dieser bestätigt werden. Es wird für das Fachpraktikum empfohlen, alle Module des ersten bis vierten Studienplansemesters bereits absolviert zu haben. Notwendige Voraussetzung ist der Nachweis von Modulen im Umfang von 110 ECTS-Leistungspunkten aus dem ersten bis vierten Studienplansemester.

(3) Das Fachpraktikum ist ein Pflichtpraktikum und richtet sich nach der Ordnung für die Durchführung des Fachpraktikums in den Bachelor- und Masterstudiengängen der HTW Berlin in der jeweils gültigen Fassung und den Richtlinien für die inhaltliche Gestaltung der praktischen Ausbildung gemäß Anlage 7.

(4) Das Fachpraktikum wird undifferenziert bewertet. Es ist erfolgreich absolviert, wenn alle Nachweise gemäß der Studien- und Prüfungsordnung für den Bachelorstudiengang Cyber Security and Business (vgl. Anlage 7) erbracht sind.

§ 12 Modulprüfungen

(1) Alle Module, mit Ausnahme des Moduls Specialist Internship, werden differenziert bewertet.

(2) Die erfolgreiche Teilnahme an einem Modul wird durch das Bestehen einer einheitlichen Modulprüfung nachgewiesen. Art, Form und Umfang der Modulprüfungen werden in den Modulbeschreibungen für den Bachelorstudiengang Cyber Security and Business festgelegt.

(3) Wird die Modulprüfung als Kombinationsprüfung gemäß § 12 Abs. 3 RStPO – Ba/Ma durchgeführt, beträgt die Gesamtpunktzahl 100, wobei die Punkteverteilung in der Modulbeschreibung auszuweisen ist.

(4) Das Bestehen der Modulprüfung ist Voraussetzung für den Erwerb von ECTS-Leistungspunkten. Die Anzahl der für die einzelnen Module festgesetzten ECTS-Leistungspunkte sind in den Anlagen 2 und 3 aufgeführt.

(5) Wird die Prüfung in einem Wahlpflichtmodul bestanden, kann das Wahlpflichtmodul nicht mehr durch ein anderes Wahlpflichtmodul ersetzt werden. Möglich ist jedoch die Ausstellung eines Leistungsnachweises über das zusätzlich absolvierte Wahlpflichtmodul durch den oder die Dozent*in.

(6) Die Zulassung zu einer Modulprüfung oder Prüfungsleistung setzt die Erstbelegung des entsprechenden Moduls gemäß Hochschulordnung voraus. Für die Wiederholung einer nicht bestandenen oder nicht angetretenen Modulprüfung ist die Prüfungsanmeldung zwingend erforderlich.

(7) Für das Modul B21 Project Sustainability in IT gibt es nur Prüfungsmöglichkeit im Semester. Für die Wiederholung der nicht bestandenen oder nicht angetretenen Modulprüfung bedarf es der erneuten Belegung des Moduls B21 Project Sustainability in IT.

§ 13 Abschlussprüfung: Bachelorarbeit

(1) Die Abschlussprüfung besteht aus der Bachelorarbeit und dem Abschlusskolloquium.

(2) Zur Bachelorarbeit wird zugelassen, wer Module im Umfang von mindestens 150 ECTS-LP aus dem ersten bis fünften Fachsemester erfolgreich abgeschlossen und das Fachpraktikum durch Praktikumsvertrag nachgewiesen hat. Ein oder eine Kandidat*in kann auch zugelassen werden, wenn er oder sie Module im Gesamtumfang von bis zu zehn ECTS-Leistungspunkten noch nicht erfolgreich abgeschlossen hat. Die Module der ersten drei Fachsemester müssen abgeschlossen sein.

(3) Der Anmeldeschluss für die Bachelorarbeit in der Fachbereichsverwaltung ist das Ende der 3. Woche des 6. Studienplansemesters. Die Zulassungen durch den Prüfungsausschuss haben spätestens bis zum Ende der 9. Woche des 6. Studienplansemesters zu erfolgen.

(4) Mit der Anmeldung oder dem Antrag auf Zulassung zur Abschlussprüfung unterbreitet der oder die Studierende einen Vorschlag für das Thema der Bachelorarbeit und für die Prüfer*innen. Der Prüfungsausschuss des Studienganges beschließt die Zusammensetzung der Prüfungskommission und legt das Thema der Abschlussarbeit sowie den Beginn und das Ende der Bearbeitungszeit schriftlich fest.

(5) Der zeitliche Bearbeitungsaufwand der Bachelorarbeit entspricht 12 ECTS-Leistungspunkten (360 Arbeitsstunden). Die Bearbeitungszeit für die Bachelorarbeit umfasst neun Wochen (in der Regel im Zeitraum Semesterwoche 10 – 19 des sechsten Fachsemesters).

(6) Die Bachelorarbeit ist fristgerecht in der Fachbereichsverwaltung in der geforderten Form gemäß § 26 Abs. 7 der RStPO – Ba/Ma in der jeweils gültigen Fassung einzureichen.

(7) Die Bachelorarbeit ist in englischer Sprache zu erstellen Die Bachelorarbeit kann als Gruppenarbeit mit zwei Personen durchgeführt werden. In jedem Fall müssen die Beiträge der einzelnen Prüflinge abgrenzbar und individuell zu beurteilen sein.

§ 14 Abschlussprüfung: Abschlusskolloquium

(1) Voraussetzung für die Zulassung zum Abschlusskolloquium sind eine mindestens mit „ausreichend“ beurteilte Bachelorarbeit und der erfolgreiche Abschluss aller Module, insgesamt im Umfang von 177 ECTS-Leistungspunkten, im Bachelorstudiengang Cyber Security and Business.

(2) Die Abschlussprüfung (Bachelorarbeit und Abschlusskolloquium) ist bestanden, wenn die Bachelorarbeit und das Abschlusskolloquium jeweils mit mindestens „ausreichend“ (4,0) bewertet wurden. Die Beurteilung der Bachelorarbeit und des Abschlusskolloquiums erfolgt jeweils differenziert durch eine Prüfungsnote gemäß der Notenskala nach § 17 Abs. 1 Spalte 2 der RStPO –

Ba/Ma in der jeweils gültigen Fassung. Die Note X_2 für die Abschlussprüfung wird nach der untenstehenden Formel berechnet. Dabei wird die errechnete Note nach den ersten beiden Stellen hinter dem Komma abgeschnitten.

$$X_2 = \frac{4}{5} X_{(21)} + \frac{1}{5} X_{(22)}$$

X_2 – Note der Abschlussprüfung

$X_{(21)}$ – Note für die Bachelorarbeit

$X_{(22)}$ – Note für das Abschlusskolloquium

(3) Das Abschlusskolloquium orientiert sich schwerpunktmäßig am Thema der Bachelorarbeit einschließlich der benachbarten und ergänzenden Wissensgebiete. Durch das Abschlusskolloquium soll festgestellt werden, ob der oder die Studierende das methodische Vorgehen und die Ergebnisse der Bachelorarbeit selbständig begründen kann und über gesichertes Wissen und Verständnis in den Fachgebieten, denen die Bachelorarbeit zuzuordnen ist, sowie über die erforderliche Präsentations- und Kommunikationskompetenz verfügt.

(4) Wurde die Bachelorarbeit als Gruppenarbeit durchgeführt, so soll das Abschlusskolloquium als gemeinsame Prüfung organisiert werden.

§ 15 Modulgruppen und Modulnoten auf dem Bachelorzeugnis

(1) Die in Absatz 2 genannten Module werden zur Bildung von Gesamtnoten für das Bachelorzeugnis zu fachspezifischen Modulgruppen mit eigenen Namen zusammengefasst. Soweit nichts anderes bestimmt ist, werden die Gesamtnoten dieser Modulgruppen durch die Bildung des gewogenen Mittels der einzelnen Modulnoten auf der Grundlage der ECTS-Leistungspunkte der einzelnen Module ermittelt.

(2) Die Module B12 Erste Fremdsprache und B18 Erste Fremdsprache 2 bilden die Modulgruppe Vertiefte Fremdsprache Englisch oder Vertiefte Fremdsprache Französisch oder Vertiefte Fremdsprache Spanisch oder Vertiefte Fremdsprache Deutsch (als Fremdsprache). Die gewählte Fremdsprache wird auf dem Bachelorzeugnis ausgewiesen.

(3) Reihenfolge der Module/Modulgruppen auf dem Bachelorzeugnis:

a) Pflichtmodule:

Programmierung

Allgemeine Informatik

Grundlagen IT-Security

Mathematik

IT-Sicherheit in Recht und Gesellschaft

Wissenschaftliches Arbeiten

Statistik

Cloud IT

Sichere Systeme

Webanwendungen/Software-Architektur

Einführung in die Betriebswirtschaftslehre

Netzwerke

Kryptologie

Datenbanken

Social Engineering

Notfall-Vorsorge und Notfall-Management

Mobile Devices

Netzwerk- und Systemsicherheit

Security Awareness

IoT-Security

Digitale Ökonomie

IT-Recht und Datenschutz

Normen, Standards & Zertifizierung

b) Vertiefung: Forensik oder KRITIS oder Distributed Ledger Technologie (DLT) oder fachspezifische Wahlpflichtmodule und Projekte

(Wahlpflichtmodul 1)

(Wahlpflichtmodul 2)

(Wahlpflichtmodul 3)

(Wahlpflichtmodul 4)

Project Sustainability in IT

c) Allgemeinwissenschaftliche Ergänzungsmodule:

Erste Fremdsprache: (Name der gewählten Fremdsprache)

AWE-Modul bzw. Teilmodule

ggf. Vertiefte Fremdsprache: (Name der gewählten Fremdsprache), ggf. Zweite Fremdsprache: (Name der gewählten Fremdsprache)

(4) Die Noten der Module

Mathematik

IT-Sicherheit in Recht und Gesellschaft

Wissenschaftliches Arbeiten

Erste Fremdsprache

AWE-Modul

werden auf dem Bachelorzeugnis ausgewiesen, gehen jedoch nicht in die Berechnung des Gesamtprädikates ein.

§ 16 Berechnung des Gesamtprädikates

(1) Das Gesamtprädikat des Abschlusses ergibt sich aus der Gesamtnote (X), die wiederum als gewichtetes arithmetisches Mittel der Teilnoten (X_1 und X_2) nach der Formel

$$X=0{,}85X_1+0{,}15X_2$$

berechnet, nach der zweiten Stelle hinter dem Komma abgeschnitten und auf eine Stelle nach dem Komma gerundet wird. Die Teilnoten sind:

a) der nach den Leistungspunkten je Modul ermittelte gewogene Mittelwert der Modulnoten, die in die Berechnung der Abschlussnote Eingang finden (Größe X_1); dabei wird die errechnete Note nach den ersten beiden Stellen hinter dem Komma abgeschnitten und

b) die Note der Abschlussprüfung (Größe X_2).

(2) Die Berechnung der Größe X_1 für das Gesamtprädikat erfolgt durch die Bildung eines gewogenen Mittels aller Module auf Grund der Anzahl der jeweiligen Leistungspunkte nach der Formel

$$X_1 = \frac{\sum(F_i \cdot a_i)}{\sum a_i}.$$

Darin bedeuten:

- F_i: Die Fachnoten der einzelnen Module.
- a_i: Die Gewichtungsfaktoren (ECTS-Leistungspunkte) der einzelnen Module.

(3) Die Gewichtungsfaktoren der einzelnen Module sind im Folgenden aufgeführt:

Nr.	Modulbezeichnung	Gewichtungsfaktor a_i
B1	Programmierung	5
B2	Allgemeine Informatik	5

B3	Grundlagen IT-Security	5
B7	Statistik	5
B8	Cloud IT	5
B9	Sichere Systeme	5
B10	Webanwendungen/Software-Architektur	5
B11	Einführung in die Betriebswirtschaftslehre	5
B13	Netzwerke	5
B14	Kryptologie	5
B15	Datenbanken	5
B16	Social Engineering	5
B17	Notfall-Vorsorge und Notfall-Management	5
B19	Mobile Devices	5
B20	Netzwerk- und Systemsicherheit	5
B21	Projekt Nachhaltigkeit in der IT	5
B22	Wahlpflichtmodul 1	5
B23	Wahlpflichtmodul 2	5
B24	Security Awareness	5
B25	IoT-Security	5
B26	Digitale Ökonomie	5
B27	IT-Recht und Datenschutz	5
B28	Normen, Standards & Zertifizierung	5
B29	Wahlpflichtmodul 3	5
B30	Wahlpflichtmodul 4	5
	Summe ECTS-Leistungspunkte	**125**

§ 17 Abschlussdokumente

(1) Die Absolvent*innen erhalten die Abschlussdokumente gemäß § 31 der Rahmenstudien- und -prüfungsordnung für Bachelor- und Masterstudiengänge - RStPO – Ba/Ma in ihrer jeweils gültigen Fassung.

(2) Auf dem Bachelorzeugnis wird ausgewiesen, dass der Studiengang in englischer Sprache absolviert wurde. Auf dem Bachelorzeugnis in deutscher Sprache werden die Modulbezeichnungen in

deutscher Sprache aufgeführt, Auf dem Bachelorzeugnis in englischer Sprache werden die Modulbezeichnungen in englischer Sprache aufgeführt. Die Verleihung des akademischen Grades Bachelor of Science wird auf der Bachelorurkunde bescheinigt.

(3) In den Anlagen 8 und 9 werden die Spezifika des Diploma Supplements in deutscher und englischer Sprache ausgewiesen

§ 18 Inkrafttreten/Veröffentlichung

Diese Ordnung tritt am Tage nach der Veröffentlichung im Amtlichen Mitteilungsblatt der HTW Berlin mit Wirkung vom 1. Oktober 2026 in Kraft.

Anlage 1 Fachgebundene Hochschulzugangsberechtigung nach § 11 Abs. 2. BerlHG

Folgende Berufsausbildungen sind insbesondere für eine Immatrikulation nach § 11 Abs. 2 BerlHG geeignet:

- Assistent*in - Informatik (allgemeine Informatik)
- Assistent*in - Informatik (Medieninformatik)
- Assistent*in - Informatik (Softwaretechnik)
- Assistent*in - Informatik (technische Informatik)
- Assistent*in - Informatik (Wirtschaftsinformatik)
- Datenverarbeitungskaufmann oder-frau
- Fachberater*in - Integrierte Systeme
- Fachberater*in - Softwaretechniken
- Fachinformatiker*in
- Fachinformatiker*in - Anwendungsentwicklung
- Fachinformatiker*in - Daten- und Prozessanalyse
- Fachinformatiker*in - Digitale Vernetzung
- Fachinformatiker*in - Systemintegration
- Informatikkaufmann oder-frau
- Informations- und Telekommunikationskaufmann oder -kauffrau
- Industriekaufmann oder-frau
- Industrietechnologe oder -technologin
- IT-System-Elektroniker*in
- IT-Systemkaufmann oder-frau
- Kfm. Ass./Wirtschaftsassistent*in - Betriebsinformatik
- Kfm. Ass./Wirtschaftsassistent*in - Informationsverarbeitung
- Kaufmann oder -frau - Digitalisierungsmanagement
- Sicherheitstechniker*in (IT)
- Kaufmann oder Kauffrau für IT-System-Management
- Kfm. Ass./Wirtschaftsassistent*in - Betriebsinformatik
- Kfm. Ass./Wirtschaftsassistent*in - Informationsverarbeitung
- Mathematisch-technische*r Assistent*in
- Mathematisch-technische*r Softwareentwickler*in

- Techn. Assistent*in - Elektronik und Datentechnik

Über die inhaltliche Vergleichbarkeit von Berufsausbildungen mit einer anderen Bezeichnung als der genannten entscheidet der Prüfungsausschuss.

Anlage 2 Studienplanübersicht

1. Fachsemester

Nr.	Modulbezeichnung	Art	LP	NSt	NV	EV	Form	SWS
B1	Programming	P	5	1a	keine	keine	SL PCÜ	3 2
B2	General Computer Science	P	5	1a	keine	keine	SL PCÜ	2 2
B3	Fundamentals of IT-Security	P	5	1a	keine	keine	SL	4
B4	Mathematics	P	5	1a	keine	keine	SL PÜ	3 1
B5	IT-Security in Law and Society	P	5	1a	keine	keine	SL	4
B6	Scientific Work	P	5	1a	keine	keine	SL PÜ	2 1
	Summe ECTS-LP Semester		**30**					

2. Fachsemester

Nr.	Modulbezeichnung	Art	LP	NSt	NV	EV	Form	SWS
B7	Statistics	P	5	1b	keine	B4	SL PCÜ	3 2
B8	Cloud IT	P	5	1a	keine	keine	SL PCÜ	2 2
B9	System Security	P	5	1b	keine	B3	SL PCÜ	3 2
B10	Web Applikation/Software Architecture	P	5	1a	keine	keine	SL PCÜ	2 2
B11	Introduction to Business Administration	P	5	1a	keine	keine	SL	4
B12	1st Foreign Language	WP	5	1a	keine	keine	PÜ	4
	Summe ECTS-LP Semester		**30**					

3. Fachsemester

Nr.	Modulbezeichnung	Art	LP	NSt	NV	EV	Form	SWS
B13	IT-Networks	P	5	1a	keine	keine	SL PCÜ	2 2
B14	Cryptology	P	5	1b	keine	B4	SL PCÜ	2 1
B15	Databases	P	5	1b	keine	B10	SL PCÜ	2 2
B16	Social Engineering	P	5	1a	keine	keine	SL PCÜ	2 2
B17	Emergency Preparedness and Management	P	5	1a	keine	keine	SL PCÜ	2 2
B18	Supplementary Elective Module	WP	5	1a	keine	keine	[1]	4
	Summe ECTS-LP Semester		**30**					

4. Fachsemester (Mobilitätssemester)

Nr.	Modulbezeichnung	Art	LP	NSt	NV	EV	Form	SWS
B19	Mobile Devices	P	5	1a	keine	keine	SL	2
B20	Network and System Security	P	5	1b	keine	B7	SL PCÜ	2 2
B21	Project Sustainability in IT	WP	5	1b	keine	B1, B11, B16, B17	PS	4
B22	Elective Module 1	WP	5	Siehe Anlage 3				4
B23	Elective Module 2	WP	5	Siehe Anlage 3				4
B24	Security Awareness	P	5	1a	keine	keine	SL	2
	Summe ECTS-LP Semester		**30**					

[1] Die Veranstaltungsform ist abhängig vom konkret angebotenen Modul bzw. Teilmodul.

5. Fachsemester

Nr.	Modulbezeichnung	Art	LP	NSt	NV	EV	Form	SWS
B25	IoT-Security	P	5	1b	keine	B20	SL PCÜ	2 2
B26	Digital Economy	P	5	1a	keine	keine	SL	4
B27	IT Law and Data Protection	P	5	1b	keine	B5	SL	4
B28	Norms, Standards and Certification	P	5	1b	keine	B5	SL	4
B29	Elective Module 3	P	5	Siehe Anlage 3				4
B30	Elective Module 4	P	5	Siehe Anlage 3				4
	Summe ECTS-LP Semester		**30**					

6. Fachsemester

Nr.	Modulbezeichnung	Art	LP	NSt	NV	EV	Form	SWS
B31	Specialist Internship Specialist Internship Seminar	P	15	1b	Siehe § 11		 PS[1]	 1
B32	Bachelor's Thesis	WP	12	1b	Siehe § 13		BA	0
B33	Bachelor’s Thesis Seminar and Final Oral Examination	P	3	1b	Siehe § 14		PS	1
	Summe ECTS-LP Semester		**30**					
	Summe ECTS-LP Studium gesamt		**180**					

[1] Findet als wöchentliches virtuelles Treffen mit medialer Unterstützung Online (E-Learning) statt.

Erläuterungen:

Form der Lehrveranstaltung:

SL	Seminaristischer Lehrvortrag	PCÜ	PC-Übung
BÜ	Begleitübung	PS	(Projekt-)Seminar
PÜ	Praktische Übung	BA	Bachelorarbeit

Art des Moduls:

P	Pflichtmodul	WP	Wahlpflichtmodul

Allgemein:

LP	ECTS-Leistungspunkte	SWS	Semesterwochenstunden
EV	Empfohlene Voraussetzung (Module mit empfohlen bestandener Prüfungsleistung)		
NV	Notwendige Voraussetzung (Module mit notwendig bestandener Prüfungsleistung)		
NSt	Niveaustufe (1a = voraussetzungsfrei/1b = voraussetzungsbehaftet)		

Anmerkungen:

Ein ECTS-Leistungspunkt steht für eine studentische Lernzeit (Workload) von 30 Stunden à 60 Minuten. Die Workload der Bachelorarbeit beträgt 12x30 Stunden = 360 Stunden. Als maximale Bearbeitungsdauer sind neun Wochen vorgesehen, so dass eine termingerechte Abgabe der Bachelorarbeit eine Durchführung des Kolloquiums zum Ende des Semesters ermöglicht.

Anlage 3 Wahlpflichtmodule

Angebot für die Wahlpflichtmodule 1 bis 4

Aus den angebotenen Modulen können im 4. und 5. Fachsemester vier Module im Umfang von 20 ECTS-Leistungspunkten gewählt werden. Studierende, die Module im Umfang von 15 ECTS aus einer Vertiefung (Forensics, CI oder DLT) erfolgreich absolviert haben, bekommen die gewählte Vertiefung im Zeugnis ausgewiesen. Andernfalls werden die gewählten Module unter „fachspezifische Wahlpflichtmodule“ im Zeugnis ausgewiesen. Die Zuordnung der Module zu den Vertiefungen und die Voraussetzungen sind in der nachfolgenden Tabelle dargestellt.

Mod.-Nr.	Modulbezeichnung	Form	SWS	NSt	NV	EV	Forensics	CI	DLT	Comprehensive[1]
B110	Forensics in Operating and Application Systems	PCÜ	4	1b	keine	B9	X			
B111	Analysis Methods for Forensic Data	PCÜ	4	1a	keine	keine	X			
B112	Forensic Psychology	PÜ	4	1a	keine	keine	X			
B113	Digital Investigation	PCÜ	4	1b	keine	B16	X			
B114	Testing & Hacking	PCÜ	4	1b	keine	B10				X
B115	Current Topics in Forensics	PÜ	4	1a	keine	keine	X			
B130	Critical Infrastructure Protection Objectives	PÜ	4	1b	keine	B3		X		
B131	Security Operation (SOC)	PCÜ	4	1b	keine	B10, B16		X		
B132	Handling Specific Risks	PÜ	4	1b	keine	B17		X		
B134	Change Management (IT & HR)	PS	4	1b	keine	B22				X
B135	Current Topics in CI	PÜ	4	1a	keine	keine		X		

[1] Module aus der Kategorie Comprehensive werden mit unter der gewählten Vertiefung ausgewiesen. Wird keine Vertiefung studiert, dann werden die Module der Kategorie Comprehensive unter „Fachspezifische Wahlpflichtmodule“ ausgewiesen.

B150	Fundamentals of Blockchain-Technology/DLT	PCÜ	4	1b	keine	B14			X	
B151	Token Economy, Cryptocurrencies and Digital Assets	PS	4	1a	keine	keine			X	
B152	Blockchain Business Development	PÜ	4	1b	keine	B15			X	
B153	Blockchain Security	PCÜ	4	1b	keine	B9			X	
B155	Current Topics in Blockchain-Technology	PÜ	4	1b	keine	B22			X	
B200	Emergency Management & Psychological Aspects	PÜ	4	1a	keine	keine				X

Anlage 4 AWE-Module/Fremdsprachen

Folgende Varianten werden für das Modul Erste Fremdsprache und das AWE-Modul angeboten:

Variante 1 (gemäß § 10 Abs. 2 S. 1 Buchstabe a) RStPO-Ba/Ma)

Variante 1a:

Nr.	Modulbezeichnung	Art	Form	SWS	LP	NSt	NV	EV
B12	Englisch Fachsprache C1.1 Wirtschaft (W) **oder** Französisch/Spanisch Fachsprache B1.2 W **oder** Deutsch[1] als Fremdsprache (mindestens auf dem Niveau der sprachlichen Anforderungen für den Hochschulzugang))	WP	PÜ	4	**5**	1a	-	-
B18	Englisch Fachsprache C1.2 W **oder** Französisch/Spanisch Fachsprache B2.1 W **oder** Deutsch als Fremdsprache (aufbauend auf dem erreichten Niveau des Moduls B12)	WP	PÜ	4	**4**	1b	-	B12

Variante 1b:

Nr.	Modulbezeichnung	Art	Form	SWS	LP	NSt	NV	EV
B12	Englisch Fachsprache C1.1 W **oder** Französisch/Spanisch Fachsprache B1.2 W	WP	PÜ	4	**5**	1a	-	-

[1] gilt nur für Studierende mit Hochschulzugangsberechtigung in einer anderen Sprache als Deutsch

	oder Deutsch[1] als Fremdsprache (mindestens auf dem Niveau der sprachlichen Anforderungen für den Hochschulzugang))							
B18	Zweite Fremdsprache	WP	PÜ	4	**5**	1a	-	-

Variante 2 (gemäß § 10 Abs. 2 S. 1 Buchstabe b) RStPO-Ba/Ma)

Nr.	Modulbezeichnung	Art	Form	SWS	LP	NSt	NV	EV
B12	Englisch Fachsprache C1.1 W **oder** Französisch/ Spanisch Fachsprache B1.2 W **oder** Deutsch[2] als Fremdsprache (mindestens auf dem Niveau der sprachlichen Anforderungen für den Hochschulzugang)	WP	PÜ	4	**5**	1a	-	-
B18	AWE-Modul (gemäß § 10 Abs. 2 S. 1 Buchstabe b) RStPO-Ba/Ma)	WP	[3]	4	**5**	1a	-	-

Variante 3 (gemäß § 10 Abs. 2 S. 1 Buchstabe c) RStPO-Ba/Ma)

Nr.	Modulbezeichnung	Art	Form	SWS	LP	NSt	NV	EV
B12	Englisch Fachsprache C1.1 W **oder** Französisch/ Spanisch Fachsprache B1.2 W **oder**	WP	PÜ	4	**5**	1a	-	-

[1] gilt nur für Studierende mit Hochschulzugangsberechtigung in einer anderen Sprache als Deutsch

[2] gilt nur für Studierende mit Hochschulzugangsberechtigung in einer anderen Sprache als Deutsch

[3] Die Form ist abhängig von den jeweiligen Angeboten.

	Deutsch[1] als Fremdsprache (mindestens auf dem Niveau der sprachlichen Anforderungen für den Hochschulzugang))							
B18	AWE-Modul (gemäß § 10 Abs. 2 S. 1 Buchstabe c)[2] RStPO-Ba/Ma)	WP	[3]	4	**5**	1a	-	-

[1] gilt nur für Studierende mit Hochschulzugangsberechtigung in einer anderen Sprache als Deutsch

[2] Der Prüfungsausschuss stellt auf Antrag des oder der Studierenden fest, ob das gewählte Modul als AWE-Modul anerkannt werden kann.

[3] Die Form ist abhängig von den jeweiligen Angeboten.

Anlage 5 Modulübersicht

Nr.	Modulbezeichnung Deutsch	Modulbezeichnung Englisch	LP
B1	Programmierung	Programming	5
B2	Allgemeine Informatik	General Computer Science	5
B3	Grundlagen IT-Security	Fundamentals of IT-Security	5
B4	Mathematik	Mathematics	5
B5	IT-Sicherheit in Recht und Gesellschaft	IT-Security in Law and Society	5
B6	Wissenschaftliches Arbeiten	Scientific Work	5
B7	Statistik	Statistics	5
B8	Cloud IT	Cloud IT	5
B9	Sichere Systeme	System Security	5
B10	Webanwendungen/Software-Architektur	Web Applikation/Software Architecture	5
B11	Einführung in die Betriebswirtschaftslehre	Introduction to Business Administration	5
B12	Erste Fremdsprache	1st Foreign Language	5
B13	Netzwerke	IT-Networks	5
B14	Kryptologie	Cryptology	5
B15	Datenbanken	Databases	5
B16	Social Engineering	Social Engineering	5
B17	Notfall-Vorsorge und Notfall-Management	Emergency Preparedness and Management	5
B18	AWE-Modul	Supplementary Elective Module	5
B19	Mobile Devices	Mobile Devices	5
B20	Netzwerk- und Systemsicherheit	Network and System Security	5
B21	Projekt Nachhaltigkeit in der IT	Project Sustainability in IT	5
B24	Security Awareness	Security Awareness	5
B25	IoT-Security	IoT-Security	5
B26	Digitale Ökonomie	Digital Economy	5
B27	IT-Recht und Datenschutz	IT Law and Data Protection	5
B28	Normen, Standards & Zertifizierung	Norms, Standards and Certification	5
B31	Fachpraktikum	Specialist Internship	15

B32	Bachelorarbeit	Bachelor's Thesis	12
B33	Bachelorseminar und Abschlusskolloquium	Bachelor’s Thesis Seminar and Final Oral Examination	3
B110	Forensik in Betriebs- und Anwendungssystemen	Forensics in Operating and Application Systems	5
B111	Analysemethoden für forensische Daten	Analysis Methods for Forensic Data	5
B112	Forensik Psychologie	Forensic Psychology	5
B113	Digitale Ermittlungen	Digital Investigation	5
B114	Testing & Hacking	Testing & Hacking	5
B115	Aktuelle Themen der Forensik	Current Topics in Forensics	5
B130	Schutzziele KRITIS	Critical Infrastructure Protection Objectives	5
B131	Security Operation (SOC)	Security Operation (SOC)	5
B132	Umgang mit speziellen Risiken	Handling Specific Risks	5
B134	Change Management (IT & HR)	Change Management (IT & HR)	5
B135	Aktuelle Themen KRITIS	Current Topics in CI	5
B150	Einführung in die Blockchain-Technologie/DLT	Fundamentals of Blockchain-Technology/DLT	5
B151	Token-Ökonomie, Kryptowährungen und digitale Vermögenswerte	Token Economy, Cryptocurrencies and Digital Assets	5
B152	Blockchain Business Development	Blockchain Business Development	5
B153	Blockchain Security	Blockchain Security	5
B155	Aktuelle Themen Blockchain-Technologie	Current Topics in Blockchain-Technology	5
B200	Krisenmanagement & psychologische Aspekte	Emergency Management & Psychological Aspects	5

Anlage 6 Lernergebnisse und Kompetenzen für jedes Modul

1. Fachsemester

B1 Programming

Lernergebnisse und Kompetenzen
Die Studierenden • können eine Problemstellung algorithmisch erfassen und in ein Programm überführen; • schreiben objektorientierte Programme unter Verwendung von Standard-Klassen; • verstehen das objektorientierte Klassenkonzept und erlernen Projekte zu modularisieren; • gewinnen einen sicheren Umgang mit Interpreter/Compiler und einer Entwicklungsumgebung; • lernen relevante Literatur und Dokumentation zu nutzen; • erlangen die Fähigkeiten, eigenständig zu lernen, technologische Grundlagen zu verstehen und praktische Lösungen für algorithmische Probleme zu finden; • können konzeptionell und strukturiert vorgehen und erlangen eine systematische Arbeitsweise; • erweitern ihre Kenntnisse zur Objektorientierung, indem sie einen sicheren Umgang mit dem Konzept der objektorientierten Vererbung, abstrakten Klassen, Interfaces und Polymorphismus erwerben; • erwerben die Fähigkeit zum Speichern und Einlesen von Daten in und aus Dateien und zum Einsatz dynamischer Datenstrukturen; • vertiefen ihre Kenntnisse zur Programmierung in ausgewählten Gebieten; • erlangen die Fähigkeit durch eigenständige und systematische Arbeitsweise komplexe Zusammenhänge zu bewältigen, sich in unbekannte Themen schnell einzuarbeiten und komplexe Implementierungsprobleme in praktische Lösungen umzusetzen.

B2 General Computer Science

Lernergebnisse und Kompetenzen
Die Studierenden • kennen die Grundprinzipien des Aufbaus eines Rechners; • kennen die in der Informatik verwendeten Zahlensysteme und Zeichentabellen und können diese den elementaren Datentypen von C zuordnen; • kennen die wichtigsten Adressierungssysteme und Grundprinzipien von Rechnernetzen; • kennen die wichtigsten Shellbefehle einer ausgewählten Linux-Shell, sowie reguläre Ausdrücke und Umgebungsvariablen; • kennen die wichtigsten Sprachelemente zum Aufbau von Shell-Skripten; • kennen die Unterschiede zwischen interpretierten und kompilierten Programmiersprachen; • sind in der Lage, Zahlensysteme ineinander umzurechnen; • können mit MAC- und IP-Adressen umgehen und einfache Netzwerkbefehle von der Shell aus ausführen; • sind fähig, z.B. ein Linux-Betriebssystem von der Shell aus zu bedienen, sowie einfache Shell-Skripte schreiben; • können interpretierte Programme starten, beispielsweise Bash-Skripte oder Python-Skripte; • können einfache Programme einer kompilierten Sprache übersetzen und zum Laufen bringen (beispielsweise C-Programme oder Java-Programme).

B3 Fundamentals of IT Security

Lernergebnisse und Kompetenzen
Die Studierenden • verstehen die Grundlagen von IT-Systemen, -Architekturen, von Netzen, IT-Infrastrukturen und Betriebssystemen mit folgenden Schwerpunkten: - Grundlagen der Informationssicherheit und IT-Sicherheit, - Ziele der IT-Sicherheit, Sicherheitsinteresse und Schutzziele, - Bedrohungen, Gefährdungen und Schwachstellen, - Rollen, Aufgaben und Funktionen, - Authentifikation und Identitäten, - Zugriffskontrolle und Berechtigungskonzepte, - IT-Sicherheitsmanagement, Konzepte und Vorgehen, - Bedeutung der IT-Sicherheit für Organisation, Personal und Technik. • kennen die Grundzüge zur Erstellung von IT-Sicherheitskonzepten; • erwerben das notwendige Systemverständnis; • verfügen über die Fähigkeit, IT-Sicherheitsmechanismen zur physischen Absicherung, Authentifikation und Zugriffskontrolle zu verstehen und wesentliche Eigenschaften zu kennen und umzusetzen.

B4 Mathematics

Lernergebnisse und Kompetenzen
Die Studierenden • sind fähig, komplexe Sachverhalte zu abstrahieren und diese formal, logisch korrekt und präzise in der Sprache der Mathematik zu beschreiben; • können die Komplexität und Machbarkeit von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen; • können mit reellen und komplexen Zahlen rechnen; • können die Lösungen von Gleichungen und Ungleichungen bestimmen; • können Grenzwerte von Folgen und Reihen bestimmen; • können rationale, trigonometrische, Potenz-, Exponential- und Logarithmus-Funktionen berechnen, ableiten und integrieren; • können mit Vektoren und Matrizen rechnen; • können lineare Gleichungssysteme aufstellen und lösen; • können einfache mathematische Modelle aufstellen und in diesen logisch schlussfolgern; • können die Korrektheit von mathematischen Sätzen durch Nachvollziehen von Beweisen beurteilen, und einfache Sätze selbst beweisen.

B5 IT Security in Law and Society

Lernergebnisse und Kompetenzen
Die Studierenden • erlangen einen Überblick über die Grundlagen des Rechtsstaats (Deutschland und Europa) und die Systematik der für die Digitalisierung relevanten, allgemeinen (Vertragstyp unabhängigen) Rechtsbereiche; • beherrschen grundlegende Begriffe des allgemeinen Zivilrechts, des allgemeinen Schuldrechts sowie weiterer relevanter Rechtsbereiche wie das Recht des geistigen Eigentums, Datenschutzrecht, das Recht der digitalen Dienste und Märkte, internationales Privatrecht, sowie IT-Sicherheitsrecht und Krypto-Regulierung; • können nach Abschluss des Moduls rechtliche Fragestellungen im Kontext der Digitalisierung erkennen und mit Hilfe der erlernten Dogmatik erste Lösungswege zu entwickeln.

B6 Scientific Work

Lernergebnisse und Kompetenzen
Die Studierenden • beherrschen Methoden des wissenschaftlichen Arbeitens; • können eigenständig Daten- und Informationen gewinnen und bewerten sowie die relevante Literatur auswählen, beschaffen und Quellen korrekt angeben; • sind mit den Vorgaben zur inhaltlichen und formalen Gestaltung schriftlicher wissenschaftlicher Arbeiten vertraut und können die Inhalte adressatengerecht präsentieren sowie wissenschaftliche Texte verfassen; • sind in der Lage komplexe Aufgabenstellungen zu definieren, strukturieren, planen (Zeit, Ressourcen, Kosten), auf unterschiedliche Teammitglieder aufzuteilen, den Fortschritt zu kontrollieren sowie die Risiken zu analysieren und Gegenmaßnahmen einzuleiten.

2. Fachsemester

B7 Statistics

Lernergebnisse und Kompetenzen
Die Studierenden erwerben • ein grundlegendes Verständnis über die Vorgehensweise der deskriptiven Statistik/Unterschied zur schließenden Statistik; • eine Übersicht über Methoden der Datenerhebung und über wichtige Datenquellen in der Wirtschafts- und Sozialstatistik; • Kenntnisse über Methoden der deskriptiven univariaten Verteilungsanalyse, Korrelations- und Regressions- sowie Zeitreihenanalyse; • Kenntnisse über Verhältniszahlen/Indexzahlen als Grundlage für die Konstruktion von Wert-, Preis- und Mengenindizes; • Kenntnisse zur Nutzung von Statistiksoftware zur Datenerhebung, Datenaufbereitung und Datenanalyse am Beispiel einer ausgewählten Statistik-Standardsoftware; • die Fähigkeit zur Vorbereitung und Durchführung computergestützter deskriptiver Datenanalysen für ausgewählte Problemstellungen unter Nutzung von Statistiksoftware.

B8 Cloud IT

Lernergebnisse und Kompetenzen
Die Studierenden • kennen die Grundlagen des Cloud Computing (vor allem Konzepte, Storagetechnologien, Container(-bau) und Serverless Computing; • sind zur ersten eigenständigen Entwicklung und Deployment mobiler Anwendungen in der Lage; • können Cloud-Einsatzszenarien und Betriebsszenarien entwickeln und wissen um die Implementierung; • können eine Virtualisierungs-Umgebung aufbauen; • können SDN (Software Defined Networks) im Could Umfeld einsetzen; • sind in der Lage, eine einfache Cloud zu erstellen.

B9 System Security

Lernergebnisse und Kompetenzen
Die Studierenden lernen die wesentlichen Merkmale über • die Grundbegriffe der Sicherheit von IT-Systemen und Netzwerken; • historische und aktuelle Angriffe und Schwachstellen; • verschiedene Angreifer-Typen und Angriffsmuster; • typische Sicherheitsrisiken; • die Gefahrenpotentiale und Sicherheitsmechanismen auf den verschiedenen Netzwerkschichten des ISO/OSI Modells (IPsec, TLS, 802.1x, RADIUS, Kerberos, OpenVPN, NATs und Firewalls); • Angriffsszenarien und Verteidigungsmöglichkeiten für Client und Server-Anwendungen; • die Risiken und Funktionsweise von Single-Sign-On Systemen; • die Wirkungsweise und Anwendung von Intrusion Detection Systemen und Honeypot Systemen. Ferner sind die Studierenden in der Lage, • adäquate Schutzmechanismen für Netzwerkkommunikation zu bestimmen; • Firewall-Systeme basierend auf Anwendungsanforderungen zu konfigurieren; • Schutzmechanismen für sichere Webkommunikation basierend auf TLS umzusetzen; • sichere Kommunikationsarchitekturen zu erstellen und umzusetzen; • Sicherheitsrisiken in bestehenden Systemen zu erkennen und gefährdete Anwendungen von anderen Anwendungen zu isolieren; • komplexe Sachverhalte zu verstehen und richtig einzuordnen; • Lösungswege zu erarbeiten; • die Methoden der Dokumentation und Präsentation zielgruppengenau einzusetzen.

B10 Web Applications / Software Architecture

Lernergebnisse und Kompetenzen
Die Studierenden kennen • die typischen Merkmale von Web-Anwendungen; • die Grundlage der HTML, XHTML; • die Grundlagen von CSS; • die Grundlagen von JavaScript und JQuery; • Client-Server-Architektur; • die Anforderungen, um eine Webanwendung von Frontend bis Backend zu konzipieren. Darüber hinaus entwickeln die Studierenden • ein fundiertes Methoden- und Fachwissen aus der Informatik und Software-Entwicklung, um Anwendungs- und Softwaresysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren; • ein Verständnis für die Anforderungen eines Kunden in Bezug auf die Struktur einer einfachen Webseite und können dieses umsetzen; • ein Verständnis über die Architektur moderner Webanwendungen.

B11 Introduction to Business Administration

Lernergebnisse und Kompetenzen

Die Studierenden verstehen
• die grundlegenden Modelle der Wirtschaftswissenschaft;
• VWL mit Netzwerk-Theorie;
• die grundlegenden Konzepte betriebswirtschaftlichen Handelns;
  o Strategie und Organisation;
  o internes und externes Rechnungswesen;
  o Controllingfunktionen;
  o Finanzierung und Investition;
  o Marketing;
  o Produktion.
Darüber hinaus können die Studierenden
• die Zusammenhänge zwischen betriebs- und volkswirtschaftlichen Entscheidungen herstellen;
• die Grundlagenkenntnisse der Unternehmensorganisation herleiten und dabei sowohl Organisationsbegriffe definieren als auch verschiedenen Funktionen von Organisationsstrukturen in den Gesamtkontext von Cyber Security and Business verorten;
• die theoretischen Grundlagen auf Praxisbeispiele anwenden.

3. Fachsemester

B13 IT-Networks

Lernergebnisse und Kompetenzen
Die Studierenden • erwerben ein generelles Verständnis für die Funktionsweise von Netzwerksystemen; • kennen die aktuellen Netzwerk-Protokolle und können die Situation im Netzwerk zu beurteilen, um das angestrebte IT-Sicherheitsniveau eines Unternehmens / Organisation sicherzustellen; • kennen die Funktionsweise von Sicherheitslösungen und bauen das Verständnis ihres Einsatzes im Betrieb und Zusammenwirkens auf; • sind in der Lage, einige dieser Lösungen selbst zu implementieren und einzusetzen. Sie können daher • Netzwerke aufbauen und analysieren; • Router und Switches konfigurieren; • Netzwerkverkehr analysieren; • Limitierungen von Netzwerktechnologien einschätzen; • Netzwerkanwendungen entwickeln.

B14 Cryptology

Lernergebnisse und Kompetenzen
Die Studierenden • kennen die vorgestellten kryptologischen und kryptografischen Verfahren und Konzepte sowie die dazugehörigen Methoden; • sind in der Lage die betrachteten Verfahren anzuwenden und gegeneinander abzuwägen; • können einfache Sicherheitsbetrachtungen anstellen; • sind fähig, das Feld der Kryptologie auch mathematisch zu durchdringen und die vorgestellten Verfahren logisch korrekt und präzise in der Sprache der Mathematik zu fassen; • können die wichtigsten Verfahren selbst implementieren. Dies beinhaltet • Klassische Verfahren der Kryptografie; • Symmetrische Verfahren (DES, AES); • Kryptographisch sichere Zufallszahlengeneratoren; • Hashing; • Primzahlen und Primzahltests; • Chinesischer Restsatz; • Asymmetrische Kryptographie; • RSA; • Digitale Zertifikate und Zertifizierungsstellen; • Diffie-Hellman; • Elliptische Kurven und ECDH-RSA; • Blockchain und digitale Währungen; • Methoden der Kryptoanalyse.

B15 Databases

Lernergebnisse und Kompetenzen
Die Studierenden • sind in der Lage, Informationsbedürfnisse umfassender betriebswirtschaftlicher Prozesse in formale Datenmodelle auf hohem Abstraktionsniveau umzusetzen und diese relational zu implementieren; • sind fähig, relationale Datenbestände mittels komplexer SQL-Abfragen auszuwerten; • sind in der Lage, Anwendungsprogramme mit Zugriff auf Datenbanksysteme zu entwickeln und gespeicherte Prozeduren zu erstellen; • lernen Architekturmuster zur Implementierung der Persistenzschicht von Anwendungen kennen und gewinnen ein Verständnis der Struktur von Datenbanksystemen; • erhalten einen Überblick über leistungssteigernde Maßnahmen, Datensicherung und Rechteverwaltung sowie ein grundsätzliches Verständnis von Transaktionen.

B16 Social Engineering

Lernergebnisse und Kompetenzen
Die Studierenden • verstehen die Grundlagen von Social Engineering, insbesondere kennen sie die häufigsten Angriffsarten und die notwendigen Schutzsysteme; • sind in der Lage, Angriffsvektoren zu analysieren und zu beurteilen und für bestehende Abwehrmaßnahmen die Qualität zu optimieren; • erwerben die Einsicht um die Begrenztheit rein technologischer Maßnahmen; • lernen Werkzeuge und Methoden, mit denen die menschlichen Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität von Hackern ausgenutzt werden, um die Betroffenen geschickt zu manipulieren; • kennen die Möglichkeiten von OSINT (Open Source Intelligence) zur Datengewinnung und • sind vertraut mit der Gewinnung von relevanten Daten aus Sozialen Netzwerken, Webseiten, Medien und anderen offenen Quellen; • können nach Abschluss des Moduls Lösungswege für klassische Probleme aufzeigen und implementieren.

B17 Emergency Preparedness and Management

Lernergebnisse und Kompetenzen
Die Studierenden • haben ein grundlegendes Verständnis über die Abläufe in Notfall-Situationen: Ereignis – Notfall – Krise; • sind in der Lage, ein Notfall-Management-Plan mitsamt den notwendigen Ressourcen aufzustellen; • können über die Alarmierung Sofortmaßnahmen einsetzen; • können Geschäftsfortführungspläne erstellen; • sind in der Lage, Notfallhandbücher und Notfallübungspläne zu schreiben; • können die notwendige Dokumentation aufsetzen und pflegen.

4. Fachsemester

B19 Mobile Devices

Lernergebnisse und Kompetenzen
Die Studierenden • kennen die Merkmale mobiler Endgeräte, Netzwerke und Protokolle; • sind in der Lage, mobile Systeme nach vorgegebener bzw. selbst erstellter Spezifikation zu entwickeln und zu testen; • kennen aktuelle Architekturen, API's und Deployment-Möglichkeiten mobiler Applikationen (z.B. Android, IOS) und sie können für den Endanwender mobile Systeme zur Verfügung stellen; • können die Kenntnisse aus Cloud IT einbringen und Kenntnisse über die entsprechenden Cloud-Architekturen und die entsprechenden Softwarelösungen für Cloud-Einsatzszenarien abzuleiten; • sind in der Lage, Einsatzszenarien für Cloud-Anwendungen zu verstehen und entsprechend zu entwickeln; • kennen die besonderen Anforderungen an mobile Anwendungen und Systeme sowie die besonderen Anforderungen an Cloud-Services aus sowohl Kunden- als auch Anbieter-Sicht; • erwerben ein fundiertes Methoden- und Fachwissen aus der Informatik und Softwareentwicklung, um betriebliche Anwendungssysteme neu zu entwickeln, zu modifizieren und in eine bestehende Anwendungsumgebung zu integrieren; • sind in der Lage, die Komplexität, die Machbarkeit, die Sicherheit und den Innovationsgrad von angestrebten Problemlösungen erkennen bzw. miteinander vergleichen zu können; • sind in der Lage, die Trends in der Entwicklung moderner Informationstechnologien in Bezug auf einen bestimmten Anwendungsbedarf zu erkennen und die notwendigen Schlüsse daraus ableiten zu können.

B20 Network and System Security

Lernergebnisse und Kompetenzen
Die Studierenden • können grundlegende Kenntnisse der Kryptologie (vgl. Modul B14) auf kryptographische Protokolle anwenden und diese im Hinblick auf Sicherheitsziele analysieren. • haben ein tiefgreifendes Verständnis von modernen kryptographischen Netzwerkprotokollen und können Angriffe auf diese nachvollziehen. • können Spezifikationen komplexer Protokolle lesen und interpretieren, um für ein gegebenes Sicherheitsniveau geeignete Konfigurationen und Algorithmen auszuwählen. • sind in der Lage, komplexe Netzwerke und Systeme zu abstrahieren, um eine Sicherheitsanalyse durchzuführen. • wenden die grundlegenden Strategien und Gegenmaßnahmen zur Absicherung von Netzwerken und Systemen selbstständig an. Die Studierenden können • geeignete Protokolle, Parameter und Algorithmen auswählen, um definierte Sicherheitsziele zu erreichen. • Netzwerke und Systeme systematisch im Hinblick auf Sicherheitsziele analysieren. • ihre Kenntnisse über Angriffstechniken nutzen, um mögliche Angriffsvektoren aufzuzeigen. • angemessene Gegenmaßnahmen auswählen, um die Sicherheit von Netzwerken und Systemen zu erhöhen.

B21 Project Sustainability in IT

Lernergebnisse und Kompetenzen
Die Studierenden sind in der Lage, • die ökologischen Auswirkungen digitaler Technologien zu analysieren und den Energie- sowie Ressourcenverbrauch von IT-Systemen im Kontext nachhaltiger Entwicklung zu erläutern; • Nachhaltigkeitsanforderungen in der Konzeption digitaler Systeme zu berücksichtigen und entsprechende Kriterien bereits in der Planungsphase eines IT-Projektes zu integrieren; • Softwarearchitekturen unter Nachhaltigkeitsaspekten zu entwerfen und zu bewerten, insbesondere im Hinblick auf Energieeffizienz, Datenvolumen, Systemkomplexität und Skalierbarkeit; • Methoden und Werkzeuge zur Messung und Analyse des Ressourcenverbrauchs von Software anzuwenden, etwa hinsichtlich Rechenleistung, Speicherbedarf, Netzwerknutzung oder Energieverbrauch; • Energieeffiziente und ressourcenschonende Implementierungsstrategien umzusetzen, beispielsweise durch optimierte Algorithmen, effiziente Datenverarbeitung oder reduzierte Datenübertragung; • Digitale Anwendungen im Hinblick auf ihren Nachhaltigkeitsbeitrag zu analysieren und zu optimieren, indem technische Lösungen systematisch bewertet und Verbesserungspotentiale identifiziert werden; • Nachhaltigkeitsaspekte in interdisziplinären Projektkontexten zu reflektieren und technische Entscheidungen unter Berücksichtigung ökologischer, ökonomischer und gesellschaftlicher Kriterien zu begründen; • Ergebnisse eines nachhaltigkeitsorientierten IT-Projekts strukturiert zu dokumentieren und zu präsentieren, einschließlich Architekturentscheidungen, Ressourcenanalysen und Optimierungsmaßnahmen.

B24 Security Awareness

Lernergebnisse und Kompetenzen
Die Studierenden • verinnerlichen, dass technische und organisatorische Maßnahmen zur Initiierung, Wahrung und Steigerung von IT-/Informationssicherheit wichtige Maßnahmen sind, aber keinen vollständigen Schutz etablieren können, wenn der Faktor Mensch in der Sicherheitskette vernachlässigt wird; • können Informationssicherheit vor dem Hintergrund des Faktors „Mensch“ und arbeitsrechtlich-regulatorischer Relevanz einordnen; • verstehen die Wirkungsweise von organisationalen Regelwerken als handlungsleitenden Strukturen; • können die Grenzen von Regelwerken klar benennen – sowohl vor dem Hintergrund der Regelwerke an sich, als auch vor dem Hintergrund typischer Angriffsmethoden (Vishing, Phishing, Social Engineering), als auch vor dem Hintergrund nicht regelbarer Verhaltensweisen in heute noch unbekannten Angriffsmethoden („unknown unknowns“); • erkennen die Notwendigkeit umfassender Sensibilisierung als Baustein unternehmensweiter Informationssicherheit; • erlernen die Prinzipien wirksamer Kommunikation und deren Einfluss auf die Wirksamkeit von Regelwerken in Organisationen; • lernen ein Set exemplarischer awarenessbildender Maßnahmen kennen und verzahnen dies kontextuell mit den Prinzipien wirksamer Kommunikation zu wirksamen Awareness-Maßnahmen und werden dadurch in die Lage versetzt, die Vielschichtigkeit von „Sensibilisierung“ anhand praktischer Beispiele zu verorten. • erlernen exemplarisch den Ablauf gelungener Awareness-Kampagnen und sind in der Lage, wirksame Awareness-Kommunikation und andere awarenessbildende Maßnahmen zu einer zielgerichteten und wirksamen Awareness-Kampagne zu orchestrieren; • lernen, mit welchen Methoden Awareness messbar werden kann und wo aktuell noch die Grenzen der Messbarkeit von Awareness liegen.

5. Fachsemester

B25 IoT-Security

Lernergebnisse und Kompetenzen
Die Studierenden • lernen aktuelle Sicherheitsthemen im Zusammenhang mit dem IoT und gängigen Sicherheitsarchitekturen kennen; • erkunden branchenübergreifend gängige IoT-Anwendungsfälle für vernetzte Fahrzeuge, Mikronetze und Unternehmensdrohnensysteme; • sind in der Lage, Bedrohungen, Schwachstellen und Risiken zu identifizieren; • lernen die gängigen IoT-Komponenten und Technologien kennen, um ihre Systeme und Geräte zu schützen; • sind in der Lage, die Integration von Datenschutzsteuerungen in die neuen IoT-Systemdesigns zu implementieren; • lernen den Umgang mit einem realen Bedrohungsszenario für IoT-Systeme und identifizieren die Risiken mit höchster Priorität; • analysieren die Datenschutzbestimmungen und -standards, die für die Sicherung von IoT-Systemen und die Geheimhaltung von Stakeholder-Informationen gelten; • setzen sich mit den Herausforderungen für den Schutz der Privatsphäre und der Abhilfemaßnahmen für das IoT auseinander, um adäquate Lösungsvorschläge unterbreiten zu können.

B26 Digital Economy

Lernergebnisse und Kompetenzen
Die Studierenden • lernen die wesentlichen Besonderheiten digitaler Märkte und die Unterschiede zu traditionellen, analogen Märkten; • sind in der Lage, grundlegende Determinanten und Herausforderungen der Internetökonomie einschätzen zu können; • können die typischen Herausforderungen eines „digitalen“ Unternehmens z.B. in Bezug auf E-Business, E-Commerce, E-Marketing skizzieren; • kennen die informationstechnischen Grundlagen zur Entwicklung von E-Business Anwendungen und Shop-Systemen und die Unterschiede im Bereich der Geschäftsmodelle für E-Commerce; • verstehen die Erfolgsfaktoren von Online Marketing, Social Shopping, M-Commerce, B2B-Auktionen und Bezahlsystemen sowie der Plattform-Ökonomie.

B27 IT Law and Data Protection

Lernergebnisse und Kompetenzen
Die Studierenden kennen die wesentlichen rechtlichen Grundlagen der IT-Sicherheit und können sie anwenden. Wesentliche Rechtsquellen sind die NIS-Richtlinie, das BSI-Gesetz, die Cybersicherheits-Verordnung und die Datenschutzgrundverordnung (Art. 32). Im Einzelnen beherrschen sie • die Anforderungen an das IT-Sicherheitsmanagement von kritischen Infrastrukturen, digitalen Diensten und Unternehmen im besonderen öffentlichen Interesse; • die Aufgaben, Befugnisse und Angebot des Bundesamtes für Sicherheit in der Informationstechnik, insbesondere im Hinblick auf Unternehmen; • die Sicherheitsanforderungen an IT-Produkte, Zertifizierung von Produkten, IT-Sicherheitskennzeichen und spezielle Anforderungen an kritische Kernkomponenten; • die speziellen Anforderungen der DSGVO an die IT-Sicherheit beim Umgang mit personenbezogenen Daten (Art. 32); • Aufgaben und Befugnisse der Datenschutzaufsicht; • Zusammenwirken von Staat und Wirtschaft bei der IT-Sicherheit; • Sektorale Rechtsvorschriften; Neben diesen Kernfragen werden weitere für die IT-Sicherheit relevante Rechtsfragen beherrscht, insbesondere • Verantwortung der Unternehmensführung; • Vertragsrechtliche und deliktsrechtliche Anforderungen an die IT-Sicherheit von Produkten, Update-Verpflichtungen; • Auswirkungen gewerblichen Rechtsschutzes auf die IT-Sicherheit; • Strafbarkeit von IT-Sicherheitsverstößen; • Zielkonflikte zwischen Schutz der IT-Sicherheit und Angriffen auf IT-Sicherheit (Hacker-Tools, Vulnerability Disclosure).

B28 Norms, Standards and Certification

Lernergebnisse und Kompetenzen
Die Studierenden • kennen die wesentlichen Normen, Standards und Gremien; • können einen Zertifizierungsprozess adäquat begleiten; • kennen die gesetzlichen Vorschriften der deutschen Rechtsprechung sowie Cybersicherheitsverordnung, BSI-Gesetz, Basel III + IV; SOX, DSGVO; • kennen die Standards mit IT-Sicherheitsaspekten wie COBIT (Kontrollziele), ITIL (Verfahrensbibliothek) IDW PS 300 (Abschlussprüfung); • kennen die ISO-Normen für Sicherheitsmaßnahmen und Monitoring (ISO/IEC 18028 [Netzwerk], ISO/IEC TR 18044 [Sicherheitsvorfälle], ISO/IEC 18043 [Auswahl eines IDS], ISO/IEC TR 15947 [Leitfaden zu IDS], ISO/IEC 15816 [Zugriffskontrolle].

6. Fachsemester

B31 Specialist Internship

Lernergebnisse und Kompetenzen
Die Studierenden • sind mit Einsatzgebieten und Einsatzanforderungen von Cyber Security and Business in der Praxis vertraut; • kennen die praktische Mitarbeit in betrieblichen Projekten; Die Studierenden • beherrschen Methoden zum wissenschaftlichen Arbeiten; • können eigenständig Daten- und Informationen gewinnen und bewerten sowie die relevante Literatur auswählen, beschaffen und Quellen korrekt angeben; • sind mit den Vorgaben zur inhaltlichen und formalen Gestaltung schriftlicher wissenschaftlicher Arbeiten vertraut und können die Inhalte adressatengerecht präsentieren sowie wissenschaftliche Texte verfassen; • sind in der Lage komplexe Aufgabenstellungen zu definieren, strukturieren, planen (Zeit, Ressourcen, Kosten), auf unterschiedliche Teammitglieder aufzuteilen, den Fortschritt zu kontrollieren sowie die Risiken zu analysieren und Gegenmaßnahmen einzuleiten.

B32 Bachelor's Thesis

Lernergebnisse und Kompetenzen
Die Studierenden haben nachgewiesen, • dass sie fähig sind, eine bestimmte Aufgabe aus ihrem Studium selbständig erfolgreich zu bearbeiten und wissenschaftlich begründet theoretische und praktische Kenntnisse zur Lösung eines Problems einzubringen; • dass sie die Fähigkeit, selbständig eine Arbeit zu einem studienrelevanten Thema zu erstellen und eine professionelle Ausarbeitung zu verfassen, haben.

B33 Bachelor's Thesis Seminar and Final Oral Examination

Lernergebnis und Kompetenzen
Die Studierenden • haben die Fähigkeit, eine wissenschaftliche Arbeit zu erstellen; • können den eigenen Arbeitsansatz und die erzielten Ergebnisse präsentieren und argumentativ begründen.

Wahlpflichtmodule

B110 Forensics in Operating and Application Systems

Lernergebnisse und Kompetenzen
Die Studierenden • können relevante Datenquellen identifizieren und relevante Daten sichern; • wissen, wie gelöschte und geänderte Daten wieder herzustellen sind; • kennen und verstehen die Vorgehensweise der IT-forensischen Untersuchung; • haben einen Überblick über die IT-Forensik und den aktuellen State-of-the-Art; • können die aktuellen Herausforderungen an die IT-Forensik einschätzen und bewerten; • kennen die Anwendungsszenarien und können die Möglichkeit der Computer Forensik nutzen; • sind in der Lage, forensisch erfasste Daten als Beweismittel gerichtsverwertbar aufzubereiten, zu dokumentieren und zu sichern. Dazu gehören die Anwendungsfelder • Cybercrime; • IT-Angriffe und deren Abwehr; • Intrusion Detection Systeme sowie eine geeignete Projektdokumentation.

B111 Analysis Methods for Forensic Data

Lernergebnisse und Kompetenzen
Die Studierenden • sind in der Lage, forensische Datenanalyse durchzuführen, um die Daten eines Unternehmens nach Vorfällen wirtschaftskrimineller Handlungen (so genannte Fraud Detection) zu untersuchen; • lernen die Analysemethoden kennen, um Datenspuren nachgehen zu können und um Täter und Tatbeteiligte zu ermitteln; • können zugrundeliegende Handlungsmuster analysieren und entsprechende Handlungsempfehlungen abgeben; • lernen die relevante Prüfsoftware kennen und einzusetzen; • können mithilfe von Malware-Analyse und Künstlicher Intelligenz darstellen, wie digitale Gefahren aufzuspüren, Netzwerke zu sichern sind und wie Straftaten aufgeklärt werden können.

B112 Forensic Psychology

Lernergebnisse und Kompetenzen
Die Studierenden • sind mit den aktuellen Aufgaben und Entwicklungen des Krisenmanagements durch Cyber-Angriffe und den psychologischen Mustern vertraut; • lernen mithilfe eines Planspiels, sich in die Rollen sowohl der Angreifer als auch der Angegriffenen hineinzuversetzen, um die jeweiligen Verhaltensweisen besser einschätzen und um entsprechende Lösungsansätze einbinden zu können.

B113 Digital Investigation

Lernergebnisse und Kompetenzen
Die Studierenden • sind in der Lage die gängigsten Handlungsfelder und Tatbegehungsmöglichkeiten zu identifizieren; • kennen die Zielsetzungen und Motivationen der Täter, um o Zugangsdaten oder persönliche Daten auszuspionieren; o Dateien und Daten zu verschlüsseln und Lösegeld zu erpressen oder o die Kontrolle über das System zu übernehmen; • lernen, Präventionsmaßnahmen aufzusetzen.

B114 Testing & Hacking

Lernergebnisse und Kompetenzen
Die Studierenden • erlernen die Werkzeuge und Methoden, mit denen digitale Spuren gesichert und analysiert werden; • kennen die Methoden beim Penetrations-Test und können eine Test-Umgebung aufbauen; • verstehen Forensische Prinzipien bei der Sicherung und Analyse digitaler Spuren; • lernen, wann und wie welche Software getestet wird, um Schäden durch Hacker abzuwenden, • können eine reproduzierbare, technische Sicherheitsanalyse von IT-Infrastrukturen durchführen. • können einen strukturierten Bericht zu den Ergebnissen einer technischer Sicherheitsanalyse von IT-Infrastruktur erstellen und die Ergebnisse präsentieren.

B115 Current Topics in Forensics

Lernergebnisse und Kompetenzen
Die Studierenden • werden mit tagesaktuellen Themen aus dem Bereich der Forensik vertraut gemacht, die sich insbesondere mit sicherheitsrelevanten Fragen auseinandersetzen; • erhalten eine Vertiefung der Grundlagen, um die tagesaktuellen Themen im Kontext besser einordnen zu können.

B130 Critical Infrastructure Protection Objectives

Lernergebnisse und Kompetenzen
Die Studierenden • können die Schutzziele der Sektoren benennen; • lernen die Anforderungen auf technischer, prozessualer und organisatorischer Ebene zu definieren; • sind mit dem BSIG vertraut; • können den Stand der Technik anhand der existierenden nationalen und internationalen Normen bestimmen.

B131 Security Operation (SOC)

Lernergebnisse und Kompetenzen
Die Studierenden • kennen die Besonderheiten von Security Operations Center (SOC) und deren Aufgabenstellung als Sicherheitsleitstelle, um den Schutz der IT-Infrastruktur eines Unternehmens oder einer Organisation sicherzustellen; • lernen, dass das SOC alle sicherheitsrelevanten Systeme wie Unternehmensnetzwerke, Server, Arbeitsplatzrechner oder Internetservices überwacht und analysiert; • lernen, dass unter anderem die Log-Dateien der einzelnen Systeme gesammelt, analysiert und nach Auffälligkeiten untersucht und wie dieses Durchzuführen ist.

B132 Handling Specific Risks

Lernergebnisse und Kompetenzen
Die Studierenden • sind in der Lage, Risiken und Zwischenfälle zu erkennen und können darauf reagieren; • verstehen die Werkzeuge und notwendigen Vorbereitungen, die zur Risikominimierung und zur Verkürzung der Reaktionszeit auf Vorfälle, Krisen und gefährliche Situationen erforderlich sind; • verstehen, wann, wie und an wen Bedenken unter Wahrung der entsprechenden Vertraulichkeit zu kommunizieren sind; • kennen die notwendigen Instrumente, um Risiko-Richtlinien zu entwickeln und insbesondere IT-relevante Risiken zu identifizieren. Dazu gehört auch, den Plan kontinuierlich zu bewerten und neu auszurichten. • können auch psychologische Aspekte berücksichtigen; • erlernen die Prinzipien wirksamer Kommunikation und deren Einfluss auf die Wirksamkeit von Regelwerken in Organisationen.

B134 Change Management (IT & HR)

Lernergebnisse und Kompetenzen
Die Studierenden • kennen die wesentlichen Methoden des Change Management und insbesondere die Besonderheiten beim IT-Change Management; • sind in der Lage, wichtige Konzepte in den Bereichen IT-Strategie, IT-Projekte, IT-Betriebe aus der gesamtunternehmerischen Perspektive darzulegen; • können anhand ihres fundierten Wissens über Konzepte und Methoden aktuelle Forschungsansätze und Entwicklungen einordnen, selbständig weiterentwickeln und entsprechend anwenden; • sind in der Lage, Steuerung des Change Management des IT-Bereichs vorzuschlagen, zu beurteilen und kritisch zu diskutieren.

B135 Current Topics in CI

Lernergebnisse und Kompetenzen
Die Studierenden • werden mit tagesaktuellen Themen aus dem Bereich der Kritischen Infrastruktur vertraut gemacht; • erwerben Einblicke in tagesaktuelle sicherheitsrelevante Fragen im Bereich KRITIS; • erhalten eine Vertiefung der Grundlagen, um die tagesaktuellen Themen im Kontext besser einordnen zu können.

B150 Fundamentals of Blockchain Technology/DLT

Lernergebnisse und Kompetenzen
Die Studierenden • verfügen über grundlegendes allgemeines Wissen und grundlegendes Fachwissen sowie prozedurales Wissen in dem Bereich der Distributed Ledger Technologien (Techniken verteilter Kassenbücher) und im Besonderen über die Blockchain-Technologie; • können die unterschiedlichen Lösungsvorschläge für Distributed Ledgers klassifizieren und erläutern; • können die unterschiedlichen Methoden zur Konsensbildung zusammenfassen und erklären; • können die möglichen Anwendungen unterschiedlicher Distributed Ledger Technologien angeben und weitere mögliche Anwendungen ableiten; • können ausgewählte Beispiele von verteilten Kontobüchern und Konsensprotokolle implementieren; • sind in der Lage, existierende und zukünftige Vorschläge für Blockchain-Technologie zu differenzieren und ihre jeweiligen Vor- und Nachteile gegenüberzustellen; • verfügen über das Wissen, für einen gegebenen Anwendungsfall zu überprüfen, ob für diesen der Einsatz einer Blockchain-Technologie sinnvoll erscheint, bzw. ob konventionelle Datenbank-Lösungen ausreichend sind.

B151 Token Economy, Cryptocurrencies and Digital Assets

Lernergebnisse und Kompetenzen
Die Studierenden sind in der Lage, • unterschiedliche Blockchain-Architekturen (z.B. UTXO vs. Accounts-basierte Systeme) vergleichend zu analysieren und hinsichtlich Skalierbarkeit, Sicherheit und Dezentralisierung einzuordnen; • komplexe Ökosysteme (z.B. DeFi-Protokolle) als vernetzte sozio-technische Systeme zu verstehen; • Token-Modelle und Krypto-Projekte mittels geeigneter Kriterien (z.B. Tokenomics, Governance, Utility) systematisch zu analysieren und zu bewerten; • Interdependenzen zwischen Kryptomärkten und traditionellen Finanzmärkten quantitativ und qualitativ zu untersuchen; • Risiken (technisch, ökonomisch, regulatorisch) mehrdimensional zu modellieren und zu bewerten. Darüber hinaus können Studierende • eigene Use Cases für Blockchain-Anwendungen konzipieren und hinsichtlich des Mehrwertes, Umsetzbarkeit und Nachhaltigkeit beurteilen; • projektspezifisch mit allen Stakeholdern kommunizieren.

B152 Blockchain Business Development

Lernergebnisse und Kompetenzen
Die Studierenden • lernen die wesentlichen Merkmale von Blockchain-Technologie und Distributed Ledger Technologie im Zusammenhang zur Prozessoptimierung kennen und können diese zielgerichtet gemäß den Anforderungen identifizieren; • verstehen die verschiedenen Blockchain-Arten und sind in der Lage, die passende Architektur zu bestimmen; • lernen die gängigen Blockchain-Komponenten und Technologien kennen, um ihre Prozesse, Systeme und Daten zu schützen; • sind in der Lage, die Integration von Datenschutzsteuerungen in die neuen Blockchain-Systemdesigns zu implementieren; • kennen die Token-Ökonomie und ihre Ausprägungen; • können auf Basis dieser Kenntnisse entscheiden, welches Token-Modell zu welchen Business-Use-Case passt und das entsprechende Framing entwerfen; • sind mit den aktuellen Aufgaben und Entwicklungen der Blockchain- und Token-Ökonomie vertraut; • können nach Abschluss des Moduls Lösungswege für die neu-Organisation von Unternehmensprozessen unter potentieller Absicherung der kritischen Daten über eine Blockchain-basierte Lösung aufzeigen und implementieren; • entwickeln sowohl die Frontend- als auch die Backend-Lösung.

B153 Blockchain Security

Lernergebnisse und Kompetenzen
Die Studierenden • lernen die Grundlagen über die Blockchain-Technologie mitsamt den verschiedenen Protokollen und Konsensmechanismen; • können zwischen Authentifikation und Identifizierung unterscheiden; • kennen die Schwachstellen von Blockchain-Netzwerken und sind in der Lage, geeignete Gegenmaßnahmen zu entwickeln; • können unterscheiden zwischen „Sybel Attacks“, „Phishing Attacks“, „Routing Attacks“ und „51% Attacks“; • sind in der Lage, eine umfassende Sicherheitsstrategie für Unternehmen zu entwickeln, die u.a. o Identitäts- und Zugriffsmanagement; o Schlüsselverwaltung; o Schutz der Daten; o Sichere Kommunikation; o Sicherheit von intelligenten Verträgen; o Transaktionsbestätigung umfasst. Dazu gehören • Governance; • relevante regulatorische Anforderungen; • Anwendung konventioneller Sicherheitskontrollen.

B155 Current Topics in Blockchain-Technology

Lernergebnisse und Kompetenzen
Die Studierenden • setzen sich mit den aktuellen Themen aus dem Bereich der DLT / Blockchain-Technologie auseinander; • lernen die Herausforderungen bei den aktuellen Themen (z.B. DeFi, NFTs, Metaverse etc.) einzuschätzen; • können die tagesrelevante Themen (z.B. DeFi, NFTs, Metaverse etc.) im Kontext der Technologie und ihren Anwendungsmöglichkeiten einordnen.

B200 Emergency Management & Psychological Aspects

Lernergebnisse und Kompetenzen
Die Studierenden • sind mit den aktuellen Aufgaben und Entwicklungen der Krisenmanagements bei Cyber-Angriffen vertraut; • kennen die Grundlagen der Risikoanalyse und können diese fall- und situationsbezogen anwenden; • verstehen die Bedeutung risikobewertungs- und managementbezogener Handlungsfelder im Kontext von Cyber Security in Organisationen; • sind in der Lage, in heterogenen Teams zu arbeiten und Führungsaufgaben wahrzunehmen; • verstehen ethische, rechtliche, soziale, psychologische und kulturelle Aspekte, Anforderungen und Herausforderungen und beherrschen Ansätze, um Konflikte und Dilemmata abzumildern; • kennen die Grundlagen der „Security Economy“ (Aspekte des Risikomanagements im Kontext zwischen Funktionalität von Wirtschaftsprozessen und Sicherheitsrisiken); • können die Ansätze der Risikobewertung und Modelle des Krisenmanagementzyklus selbständig auf Fallbeispiele und Szenarien anwenden; • besitzen Umsetzungskompetenz zwischen der Identifikation von auf kritische Infrastruktur bezogenen Gefährdungen und der Begegnung systemspezifischer Risiken unter Berücksichtigung vorhandener Sicherheitskulturen.

AWE-Module/Fremdsprachen

B12 Erste Fremdsprache

Englisch Fachsprache C1.1 W **oder** Französisch/Spanisch Fachsprache B1.2 W **oder** Deutsch[1] als Fremdsprache (mindestens auf dem Niveau der sprachlichen Anforderungen für den Hochschulzugang))
Lernergebnisse und Kompetenzen
Englisch Fachsprache C1.1 Wirtschaft Die Studierenden • vervollkommnen bereits erworbene fachsprachliche Kenntnisse auf dem Gebiet Wirtschaft, • entwickeln auf dieser Grundlage alle Sprachfertigkeiten (Hören, Sprechen, Lesen, Schreiben) weiter, • verstehen ein breites Spektrum anspruchsvoller und umfangreicher Texte und erfassen dabei auch implizite Bedeutungen, • können sich spontan und fließend ohne größeres Suchen nach adäquaten Wendungen ausdrücken, • gebrauchen die Sprache flexibel und wirksam im sozialen, akademischen und beruflichen Kontext, • können sich klar, gut strukturiert und detailliert zu komplexen Sachverhalten äußern und dabei verschiedene Mittel zur Textverknüpfung angemessen verwenden. Französisch/Spanisch Fachsprache B1.2 Wirtschaft Die Studierenden • werden in die Fachsprache Wirtschaft eingeführt, • entwickeln auf Grundlage bereits erworbener allgemeinsprachlicher Kenntnisse alle Sprachfertigkeiten (Hören, Sprechen, Lesen, Schreiben) weiter, • verstehen den wesentlichen Inhalt klarer standardisierter Informationen zu vertrauten Themen aus den Bereichen Arbeit, Schule, Studium usw., • erwerben Kommunikationsfähigkeit in anzunehmenden Gesprächssituationen in Ländern, in denen die Sprache gesprochen wird, • können sich einfach und zusammenhängend über vertraute Fachthemen oder Themen von persönlichem Interesse äußern, • können über Erfahrungen und Ereignisse berichten sowie Träume, Hoffnungen und Ziele beschreiben, • können kurze Erklärungen und Begründungen zu Plänen und Ansichten geben. Deutsch[2] als Fremdsprache Die Studierenden erlangen in Abhängigkeit der vorhandenen Vorkenntnisse (mindestens auf dem Niveau der sprachlichen Anforderungen für den Hochschulzugang)) allgemein- und/oder fachsprachliche Kenntnisse in allen Sprachfertigkeiten (Hören, Sprechen, Lesen, Schreiben).

B18 Erste Fremdsprache 2

Englisch Fachsprache C1.2 W **oder** Französisch/Spanisch Fachsprache B2.1 W **oder** Deutsch als Fremdsprache (aufbauend auf dem erreichten Niveau des Moduls B12)
Lernergebnisse und Kompetenzen
Englisch Fachsprache C1.2 Wirtschaft Die Studierenden • erlangen sehr hohe fachsprachliche Kompetenz auf dem Gebiet Wirtschaft, • entwickeln aufbauend auf dem Modul Erste Fremdsprache 1 alle Sprachfertigkeiten (Hören, Sprechen, Lesen, Schreiben) weiter, • verstehen ein breites Spektrum anspruchsvoller und umfangreicher Texte und erfassen dabei auch implizite Bedeutungen, • können sich spontan, sehr flüssig und genau ausdrücken, • gebrauchen die Sprache flexibel und wirksam im sozialen, akademischen und beruflichen Kontext, • können sich klar, gut strukturiert und detailliert zu komplexen Sachverhalten äußern und dabei verschiedene Mittel zur Textverknüpfung angemessen verwenden, • lernen, auch bei komplexeren Sachverhalten feinere Bedeutungsnuancen deutlich zu machen. Französisch/Spanisch Fachsprache B2.1 Wirtschaft Die Studierenden • erlangen weitere fachsprachliche Kompetenz auf dem Gebiet Wirtschaft, • entwickeln aufbauend auf dem Modul Erste Fremdsprache 1 alle Sprachfertigkeiten (Hören, Sprechen, Lesen, Schreiben) weiter, • verstehen die Hauptinhalte komplexer Texte zu konkreten und abstrakten Themen, • verstehen und präsentieren relevante Themen im eigenen Fachgebiet, • können angemessen flüssige Gespräche führen, • können Texte zu einer Reihe fachlicher Themen klar und detailliert verfassen, • können den eigenen Standpunkt zu einem fachlichen Thema darlegen. Deutsch als Fremdsprache Die Studierenden • erlangen weitere allgemein- und/oder fachsprachliche Kompetenz,

[1] gilt nur für Studierende mit Hochschulzugangsberechtigung in einer anderen Sprache als Deutsch gemäß § 9 Abs. 4

[2] gilt nur für Studierende mit Hochschulzugangsberechtigung in einer anderen Sprache als Deutsch gemäß § 9 Abs. 4

- entwickeln aufbauend auf dem Modul Erste Fremdsprache alle Sprachfertigkeiten (Hören, Sprechen, Lesen, Schreiben) weiter.

B18 Zweite Fremdsprache (nicht B12)

Lernergebnisse und Kompetenzen
Die Studierenden erlangen in Abhängigkeit der vorhandenen Vorkenntnisse allgemein- und/oder fachsprachliche Kenntnisse in allen Sprachfertigkeiten (Hören, Sprechen, Lesen, Schreiben) entsprechend der von ihnen frei aus dem Angebot der ZE FS gewählten Fremdsprache und Niveaustufe (A1 bis C1.2).

B18 AWE-Modul

Lernergebnisse und Kompetenzen
Die Studierenden • erwerben überfachliche bzw. fachübergreifende, insbesondere soziale und kommunikative Kompetenzen („soft skills“) und/oder • gewinnen vertieften Einblick in geistes-, kommunikations-, gesellschafts- und kulturwissenschaftliche Denk- und Herangehensweisen und/oder • sind nach Abschluss des Moduls in der Lage, andere Kulturen besser zu verstehen und in anderen kulturellen Kontexten zu agieren und/oder • gewinnen vertiefte Einblicke in die Potenziale und Probleme interdisziplinärer wissenschaftlicher Kooperation.

Anlage 7 Richtlinien für das Fachpraktikum im Bachelorstudiengang Cyber Security and Business

§ 1 Ausbildungsbereiche und -inhalte

(1) Das Fachpraktikum ist Pflichtbestandteil des Studiums. Es kann in englischer oder deutscher Sprache im In- und Ausland absolviert werden. Die Studierenden werden durch die mehrwöchige Mitarbeit in einem Unternehmen mit den Aufgaben aus dem Bereich Wirtschafts-Informationssicherheit vertraut gemacht. Sie sollen ihr Methoden- und Prozesswissen in Praxissituationen zur erfolgreichen Lösung typischer Aufgabenstellungen der Cyber Security and Business einsetzen. Daneben sollen sie Einblicke in die technischen, organisatorischen, ökonomischen und sozialen Zusammenhänge der betrieblichen Abläufe erhalten.

(2) Die Studierenden können in allen Tätigkeitsfeldern der Cyber Security and Business in Unternehmen aller Branchen, in der Verwaltung und in Institutionen eingesetzt werden. Dies umfasst beispielsweise Aufgabengebiete der kritischen Infrastruktur, der forensischen Analyse digitaler Spuren, der IT-Security-Beratung und dem Einsatz von verteilten Netzen zur Sicherung von Daten, des Datenschutzes etc. In Zweifelsfällen entscheidet der oder die Praxisbeauftragte, ob eine vorgeschlagene Tätigkeit diesem Einsatzbereich zugeordnet werden kann.

§ 2 Dauer und Durchführung des Fachpraktikums

(1) Das Fachpraktikum findet in der Regel von der 24. Woche des fünften Fachsemesters bis Ende der neunten Woche des sechsten Fachsemesters statt, auf Antrag kann das Fachpraktikum bereits nach dem ersten Prüfungszeitraum des fünften Fachsemesters begonnen werden. Es umfasst einen Zeitraum von mind. zwölf Wochen in der Regel zu je 37,5 Stunden. Diese 450 Stunden entsprechen einem studentischen Workload von 15 ECTS-Leistungspunkten (15•30 Stunden = 450 Stunden). In begründeten Ausnahmefällen ist eine Abweichung von einem Arbeitstag nach unten möglich. Hierüber entscheidet der oder die Praxisbeauftragte des Bachelorstudienganges Cyber Security and Business. Notwendige Voraussetzung ist der Nachweis von 110 ECTS-Leistungspunkten von Modulen aus dem ersten bis viertem Studienplansemester.

(2) Die Lehrveranstaltung "Specialist Internship Seminar" findet als regelmäßiges virtuelles Treffen mit medialer Unterstützung (E-Learning) statt.

§ 3 Betreuung und Nachweise

(1) Der oder die Praxisbeauftragte des Bachelorstudienganges Cyber Security and Business betreut die Studierenden hinsichtlich Vorbereitung, Durchführung und Auswertung des Fachpraktikums.

(2) Für die erfolgreiche Durchführung des Fachpraktikums sind folgende Nachweise erforderlich:

- Zulassungsantrag und Genehmigung des Praktikums vor Beginn;

- Vom/von der Praxisbeauftragten entgegengenommener Praktikumsvertrag zwischen dem/der Studierenden und dem Praktikumsbetrieb;
- Zeugnis des Praktikumsbetriebs über eine erfolgreiche Durchführung des Praktikums;
- schriftlicher, vom Praktikumsbetrieb unterschriebener Praxisbericht, aus dem der zeitliche Ablauf des Praktikums, die Praxisaufgaben und die Tätigkeiten zur Lösung der Aufgaben hervorgehen.

(3) Das Praktikum wird undifferenziert durch den oder die Praxisbeauftragte*n bewertet.

Anlage 8 Spezifika des Diploma Supplements in deutscher Sprache

1. ANGABEN ZUM INHABER/ZUR INHABERIN DER QUALIFIKATION

1.1 Familienname(n)/1.2 Vorname(n)

1.3 Geburtsdatum (TT/MM/JJJJ)

1.4 Matrikelnummer oder Code zur Identifizierung des/der Studierenden (wenn vorhanden)

2. ANGABEN ZUR QUALIFIKATION

2.1 Bezeichnung der Qualifikation und (wenn vorhanden) verliehener Grad (in der Originalsprache)

Bachelor of Science, B.Sc.

2.2 Hauptstudienfach oder -fächer für die Qualifikation

Cyber Security and Business

mit den Vertiefungen:

Forensik oder

KRITIS oder

Distributed Ledger Technologie

2.3 Name und Status (Typ/Trägerschaft) der Einrichtung, die die Qualifikation verliehen hat (in der Originalsprache)

Hochschule für Technik und Wirtschaft Berlin, Fachhochschule (FH)

University of Applied Sciences / staatlich

2.4 Name und Status (Typ/Trägerschaft) der Einrichtung (falls nicht mit 2.3 identisch), die den Studiengangdurchgeführt hat (in der Originalsprache)

2.5 Im Unterricht/in der Prüfung verwendete Sprache(n)

Englisch

3. ANGABEN ZU EBENE UND ZEITDAUER DER QUALIFIKATION

3.1 Ebene der Qualifikation

Erster berufsqualifizierender Hochschulabschluss an einer Fachhochschule (siehe Abschnitte 8.1 und 8.4.1) inklusive einer Bachelorarbeit

3.2 Offizielle Dauer des Studiums (Regelstudienzeit) in Leistungspunkten und/oder Jahren

Regelstudienzeit:	6 Semester, 3 Jahre
Workload:	5.400 Stunden
Leistungspunkte (LP) nach ECTS:	180 LP
davon Fachpraktikum	15 LP
und Bachelorarbeit	12 LP

3.3 Zugangsvoraussetzung(en)

- allgemeine Hochschulreife oder Fachhochschulreife oder Hochschulzugangsberechtigung nach § 11 Abs. 1 oder 2 Berliner Hochschulgesetz (s. Abschnitt 8.7) und
- Englischkenntnisse der Niveaustufe C1 des Gemeinsamen Europäischen Referenzrahmen für Sprachen (GER)

4. ANGABEN ZUM INHALT DES STUDIUMS UND ZU DEN ERZIELTEN ERGEBNISSEN

4.1 Studienform

Vollzeitstudium, Präsenzstudium

4.2 Lernergebnisse des Studiengangs

Das Bachelorstudium vermittelt den Studierenden die Fähigkeit, komplexe Informatikanwendungen im Bereich der Informationssicherheit zu konzipieren, zu entwickeln und weiterzuführen. Die Pflichtmodule decken grundlegende Prinzipien, Methoden, Modelle und Werkzeuge der Informatik und Informationssicherheit ab und befähigen zur integrativen Analyse sowie zur Realisierung sicherheitsorientierter Informations- und Kommunikationssysteme. Dabei wird auch der Einfluss des Faktors Mensch auf sicherheitsrelevante Prozesse berücksichtigt.

Im Vertiefungsstudium erwerben die Studierenden umfassende Kenntnisse der Informatik, Informationssicherheit und Betriebswirtschaftslehre. Sie werden befähigt, informationsverarbeitende Systeme zu planen, einzuführen, zu betreiben, zu warten und zu verwalten. Darüber hinaus verfügen sie über fundierte Kompetenzen in Informationssicherheit und IT-Forensik, arbeiten präventiv an der Absicherung bestehender Systeme, erkennen sicherheitsrelevante Angriffe und können Untersuchungen zu Sicherheitsvorfällen durchführen.

Das Studium bereitet auf berufliche Tätigkeiten vor, die technische, wirtschaftliche, soziale und ethische Aspekte der IT-Sicherheit berücksichtigen. Die Studierenden erwerben die Fähigkeit zu selbstständiger wissenschaftlicher Arbeit, zur Anwendung wissenschaftlicher Methoden im beruflichen Kontext sowie zu kritischem Denken und verantwortungsbewusstem Handeln.

Ein weiterer Schwerpunkt liegt auf der Befähigung zum Arbeiten in internationalen Kontexten. Dies umfasst Module wie z. B. Digitale Ökonomie und Cloud IT, eine Fremdsprachenausbildung sowie die Auseinandersetzung mit globalen Standards, internationalen IT-Sicherheitsanforderungen und Besonderheiten internationaler Software- und Netzwerkumgebungen. Die Studierenden reflektieren ökologische, ökonomische und soziale Auswirkungen digitaler Technologien und berücksichtigen Aspekte der Nachhaltigkeit im Bereich Cyber Security.

Die erworbenen Kompetenzen qualifizieren die Absolvent*innen insbesondere für Tätigkeiten in den Bereichen Wirtschafts- und IT-Sicherheit (Security und Safety), IT-Sicherheit in kommunalen Einrichtungen, IT-Sicherheit und Forensik sowie IT-Sicherheit im Umfeld von Distributed-Ledger-Technologien.

Studienzusammensetzung:

Pflichtmodule:	118 ECTS-LP
optionale Wahlpflichtmodule (ohne minimale Fremdsprachenausbildung) :	35 ECTS-LP
minimale Fremdsprachenausbildung:	5 ECTS-LP
Fachpraktikum:	15 ECTS-LP
Bachelorarbeit inklusive Kolloquium:	15 ECTS-LP

4.3 Einzelheiten zum Studiengang, individuell erworbene Leistungspunkte und erzielte Noten

Siehe „Bachelorzeugnis“ für weitere Details zu den absolvierten Schwerpunktfächern und dem Thema der Bachelorarbeit inklusive ihrer Benotungen.

4.4 Notensystem und, wenn vorhanden, Notenspiegel

4.5 Gesamtnote (in Originalsprache)

– Abschlussprädikat (ungerundete Gesamtnote) –

Zusammensetzung des Gesamtprädikats:

85 % Modulnoten

15 % Abschlussprüfung (Bachelorarbeit und Abschlusskolloquium)

5. ANGABEN ZUR BERECHTIGUNG DER QUALIFIKATION

5.1 Zugang zu weiterführenden Studien

Der Abschluss berechtigt zur Aufnahme eines Masterstudiums; die jeweilige Zugangs- und Zulassungsordnung kann zusätzliche Voraussetzungen festlegen. (s. Abschnitt 8)

5.2 Zugang zu reglementierten Berufen (sofern zutreffend)

k.A.

6. WEITERE ANGABEN

6.1 Weitere Angaben

Der Studiengang ist akkreditiert und trägt das Siegel des Akkreditierungsrats (siehe unter: www.akkreditierungsrat.de).

6.2 Weitere Informationsquellen

Webseite: https://cyber-security-business.htw-berlin.de/

HTW Berlin: http://www.HTW-Berlin.de

Anlage 9 Spezifika des Diploma Supplements in englischer Sprache

1. INFORMATION IDENTIFYING THE HOLDER OF THE QUALIFICATION
1.1 Family name(s)/1.2 First name(s)
1.3 Date of birth (dd/mm/yyyy)
1.4 Student identification number or code (if applicable)

2. INFORMATION IDENTIFYING THE QUALIFICATION
2.1 Name of qualification and (if applicable) title conferred (in original language)
Bachelor of Science (B.Sc.)
2.2 Main field(s) of study for the qualification
Cyber Security and Business with the specialisations: forensics or CI or Distributed Ledger Technology
2.3 Name and status of awarding institution (in original language)
Hochschule für Technik und Wirtschaft Berlin (HTW Berlin) (University of Applied Sciences, / public)
2.4 Name and status of institution (if different from 2.3) administering studies (in original language)
2.5 Language(s) of instruction/examination

English

3. INFORMATION ON THE LEVEL AND DURATION OF THE QUALIFICATION

3.1 Level of the qualification

First degree at a university of applied sciences level (see sections 8.1 and 8.4.2), includes a bachelor thesis.

3.2 Official duration of programme in credits and/or years

Regular study period:	6 semesters, 3 years
Workload:	5,400 hours
Credits (ECTS):	180 Cr
of which specialist internship	15 Cr
and Bachelor's thesis	12 Cr

3.3 Access requirement(s)

- General university/university of applied sciences entry qualifications or university entry qualification in accordance with § 11, paras. 1 or 2 of the Berlin Higher Education Act (see section 8.7) and
- English proficiency at the C1 level of the Common European Framework of Reference for Languages (CEFR)

4. INFORMATION ON THE PROGRAMME COMPLETED AND THE RESULTS OBTAINED

4.1 Mode of study

Full-time, on-campus programme

4.2 Programme learning outcomes

The Bachelor’s programme equips students with the ability to design, develop and further advance complex IT applications in the field of information security. The compulsory modules provide fundamental principles, methods, models and tools of computer science and information security, enabling students to conduct integrative analyses and to implement security-oriented information and communication systems. The programme also addresses the role of human factors in security-related processes.

In the advanced study phase, students acquire comprehensive knowledge in computer science, information security and business administration. They are qualified to plan, implement, operate,

maintain and manage information-processing systems. Furthermore, they gain in-depth competencies in information security and IT forensics, allowing them to work preventively on securing existing systems, detect security incidents and conduct investigations of cyberattacks.

The programme prepares students for professional activities that require consideration of technical, economic, social and ethical aspects of IT security. They develop the ability to work independently using scientific methods, apply academic knowledge in professional contexts, think critically and act responsibly within society.

Another focus is on the ability to work in international contexts. This includes modules such as Digital Economy and Cloud IT, foreign language training, as well as engagement with global standards, international IT security requirements, and the specifics of international software and network environments. Students reflect on the ecological, economic, and social impacts of digital technologies and consider aspects of sustainability in the field of cyber security.

The acquired competencies qualify graduates for professional roles in business and IT security (security and safety), IT security in public administration, IT security and forensics, and IT security in the context of distributed-ledger technologies.

Programme components:

Compulsory modules:	118 ECTS Cr
optional elective modules (without minimum foreign language training):	35 ECTS Cr
Minimum foreign language training:	5 ECTS Cr
Specialist internship:	15 ECTS Cr
Bachelor’s thesis including final oral examination	15 ECTS Cr

4.3 Programme details, individual credits gained and grades/marks obtained

See the “Bachelor’s Degree Grade Transcript” for further details regarding areas of specialisation and the Bachelor’s thesis topic, including grades.

4.4 Grading system and, if available, grade distribution table

4.5 Overall classification of the qualification (in original language)

- Final grade (unrounded final mark) -

Composition of the overall grade

85% module marks

15% final examination (bachelor's thesis and final oral examination)

5. INFORMATION ON THE FUNCTION OF THE QUALIFICATION

5.1 Access to further study

This degree entitles the holder to pursue a Master’s degree; the respective Eligibility and Admission Regulations may stipulate additional requirements. (see section 8)

5.2 Access to a regulated profession (if applicable)

not specified

6. ADDITIONAL INFORMATION

6.1 Additional information

The programme is accredited and bears the seal of the Accreditation Council (see: www.akkreditierungsrat.de).

6.2 Further information sources

Website: https://cyber-security-business.htw-berlin.de/

HTW Berlin website: http://www.HTW-Berlin.de

HOCHSCHULE FÜR TECHNIK UND WIRTSCHAFT BERLIN

Study and Examination Regulations for the English-language Bachelor's degree programme

Cyber Security and Business (CSB)

Bachelor of Science (B.Sc.)

at the School of Computing, Communication and Business

from the 15th of April 2026

On the basis of § 16, section 1, no. 1 of the Statutes of the Hochschule für Technik und Wirtschaft Berlin (HTW Berlin) dated the 16th of December 2024 (HTW Berlin Official Information Circular No. 12/25) in connection with § 31 of the BerlHG in the edition released on the 26th of July 2011 (Law and Official Gazette p. 378), last legally amended on the 21st of January 2026 (Law and Official Gazette p. 23), the Faculty Council of the School of Computing, Communication and Business at HTW Berlin passed the following Study and Examination Regulations for the Bachelor's degree programme Cyber Security and Business on the 15th of April 2026[1]:

Regulation Contents

[1]Confirmed by the Executive Committee of HTW Berlin on the 13th of May 2026. (Only the original German version is binding).

§ 1 Application and Scope

(1) These Study and Examination Regulations apply to all those who, after said regulations have come into force, are enrolled as first semester students of Cyber Security and Business in the aforementioned English-language Bachelor's degree programme at the School of Computing, Communication and Business.

(2) These Study and Examination Regulations also apply for all students who, after changing university or study programme, are placed on the programme at the same stage as those in section 1 as a result of the accreditation of prior learning and examinations.

(3) The Study and Examination Regulations are supplemented by the Eligibility and Admission Regulations for the English-language Bachelor's degree programme Cyber Security and Business in their currently valid edition.

§ 2 Validity of Framework Regulations

The University Regulations of HTW Berlin (HO) in the currently valid edition, the Study and Examination Framework Regulations for Bachelor's and Master's degree programmes of HTW Berlin (Study and Examination Framework Regulations for Bachelor's and Master's degree programmes, or *RStPO - Ba/Ma*) in the currently valid edition, and the Regulations for the Implementation of the Specialist Internship in the Bachelor's and Master's degree programmes of HTW Berlin (Regulations for Implementation, or *Praxisordnung - PraxO*) in the currently valid edition form an integral part of these regulations.

§ 3 Allocation of Study Places

The allocation of study places is performed according to the BerlHG, the Berlin Higher Education Admissions Act (*Berliner Hochschulzulassungsgesetz - BerlHZG*) and the Berlin Higher Education Admissions Regulation (*Berliner Hochschulzulassungsverordnung - BerlHZVO*) in their respective valid editions in connection with the University Regulations and the Regulations on Selection Procedures for Bachelor's Degree Programmes in the currently valid edition, as well as the Eligibility and Admissions Regulations for the English-language Bachelor's degree programme Cyber Security and Business.

§ 4 Subject-Specific Higher Education Entrance Qualification

(1) In the case of applications on the basis of § 11, section 2 BerlHG, the professional qualifications listed in Annex 1 are considered particularly suitable for the Bachelor's degree programme Cyber Security and Business.

(2) The Examination Board of the degree programme shall decide on the content-related comparability of professional qualifications attained by applicants other than those listed in Annex 1.

§ 5 Qualification Objectives

(1) The aim of the Bachelor's degree programme is to train graduates who are able to design, implement and further develop complex computer science applications in the field of information security, leading to the attainment of a Bachelor of Science degree. To this end, the compulsory modules teach fundamental principles, methods, models and tools that enable students to analyse and implement security-oriented information and communication systems in terms of hardware and software in a holistic, integrative manner. Students are also sensitised to the importance of the 'human factor' in this context. By integrating the relevant fundamentals of computer science, information security and business administration, the specialisation year aims to develop the knowledge and mindset required to design, develop, introduce, use, maintain and manage information processing systems. Students gain in-depth knowledge of information security and IT forensics, which they use to work preventively to secure existing systems. They also detect attacks and take responsibility for investigating security incidents.

(2) Teaching and studies in the Bachelor's degree programme Cyber Security and Business at HTW Berlin should prepare students for professional activities, taking into account changes in the professional world and the social environment; in addition to IT security, this also includes economic, social and ethical aspects. The knowledge, skills and methods required in the process should be taught to students in such a way that they are able to carry out independent scientific work, in particular to apply scientific methods and findings in their profession and to think critically and act responsibly in society.

(3) A central aim of the degree programme is to enable students to operate in international contexts. The degree programme is therefore characterised by specialist modules with international content, such as digital economics, cloud IT and mobile devices, as well as foreign language training. Students are equipped to critically reflect on the environmental, economic and social implications of their actions and to make responsible decisions. Particularly in the context of information technology and cyber security, the knowledge of sustainability that needs to be acquired is significant, as digital systems, infrastructure and data-driven applications play a key role in resource use, energy consumption and social change. Additionally, the special features of IT security in an international context (internationalisation of software, international standards, global media and networks, etc.) are addressed.

(4) The overall aim of the programme is to equip graduates with the professional and personal skills to work primarily in the following areas:

- Economic and IT security (in the sense of security and safety)
- Business and IT security for municipal organisations (administration)
- Economic and IT security and forensics
- Economic and IT security and distributed ledger technology.

§ 6 Regular Study Period, Programme Plan, Modules

(1) The Bachelor's degree programme Cyber Security and Business is offered in English.

(2) The Bachelor's degree programme is an on-campus programme with a duration of six semesters (standard period of study). The Bachelor's degree programme comprises 180 ECTS credits. One ECTS credit corresponds to a student workload of 30 hours. The annual workload for the Bachelor's degree programme Cyber Security and Business is 1,800 hours.

(3) The programme is structured according to the Programme Plan in Annex 2 and employs a modular format as per § 4 of the Study and Examination Framework Regulations (RStPO-Ba/Ma). It contains a list of all modules included within the Bachelor's degree programme Cyber Security and Business. For each module, the curriculum specifies module designation, level, form and type (compulsory/elective), attendance time (in weekly study hours), basic learning time in terms of ECTS credits awarded and the compulsory and recommended prerequisites. The elective modules are listed in Annex 3, while the options for supplementary modules/foreign languages are set out in Annex 4

(4) Learning outcomes and skills for each module are also set out in Annex 6 and form part of these regulations.

(5) Comprehensive module descriptions are provided in the module descriptions handbook for the Bachelor's degree programme Cyber Security and Business.

§ 7 Programme Structure

(1) The Bachelor's degree programme Cyber Security and Business begins once a year in the winter semester.

(2) The fourth semester is intended as a mobility semester for studying at another university in Germany or abroad.

(3) Students are permitted to complete an interdisciplinary project (offered in English) from one of the faculties at HTW Berlin, subject to availability, this instead of a curricular elective module (B22, B23, B29 or B30) worth five ECTS credit points.

(4) Elective modules are offered in the 4th and 5th semesters. An overview of the elective modules with the assignment to the specialisations can be found in Annex 3.

Students must complete modules totalling 20 ECTS credits from the selection of elective modules offered. If modules totalling 15 ECTS credits are completed within a specialisation, this specialisation will be indicated on the Bachelor's degree certificate. Otherwise, the modules will be listed as subject-specific elective modules on the Bachelor's degree certificate.

The programme representative decides which modules are offered in a timely manner. The Faculty Council may decide on further elective modules according to current developments.

(5) In each semester, one module (amounting to five ECTS credits) may be offered as an e-learning module. This e-learning module is decided by the Faculty Council prior to the start of each semester.

All modules, with the exception of the supplementary and first foreign language modules, can be completed as e-learning modules.

(6) The programme is deemed completed when all modules, including the Bachelor's thesis and final oral examination, have been passed successfully.

§ 8 Extracurricular Studies

As part of the Extracurricular Studies programme, modules are available that are designed to develop foreign language, interdisciplinary or cross-disciplinary skills in accordance with § 2 of the RStPO-Ba/Ma in the currently valid edition.

§ 9 Extracurricular Studies: Compulsory Foreign Language Programme

(1) The Bachelor's programme includes compulsory foreign language teaching worth five ECTS credits. Foreign language programmes serve to deepen existing knowledge of a foreign language.

(2) Students select English, French or Spanish as their first foreign language. The programme is worth five ECTS credits and comprises four weekly study hours. Training in business terminology for the first chosen foreign language begins in English at a CEFR level of at least C1.1 and/or C1.2., and in other foreign languages at least at CEFR level B1.2.

(3) Students who have obtained their higher education entrance qualification in a language other than German may choose to study German as a foreign language (at a level meeting at least the language requirements for university admission) as part of the prescribed foreign language programme.

(4) The language of the student's higher education entrance qualification is excluded from the choice.

§ 10 Extracurricular Studies: Supplementary Modules

The supplementary modules amount to five ECTS credits[1]. The supplementary module can be selected freely from the German and English-language supplementary programmes offered by HTW Berlin. Regulations in accordance with § 10 of the RStPO-Ba/Ma in the currently valid edition apply. The possible options are set out in Annex 4.

[1] It is also possible to complete two sub-modules, each worth two and a half credits.

§ 11 Specialist Internship

(1) In addition to the subjects listed in the Programme Plan in Annex 2, the Bachelor's degree programme includes a specialist internship amounting to 15 ECTS credits, which usually begins in the 24th week of the 5th semester. It lasts for 12 weeks and must be completed as a full-time internship.

(2) Students should apply to the internship coordinator of the degree programme for admission to the internship in good time before starting it, as confirmation by the aforementioned individual is required. The University recommends that students have completed all modules in the first to fourth semesters before embarking on the specialist internship. The necessary prerequisite is proof of having completed modules totalling 110 ECTS credits from the first to the fourth semesters of the degree programme.

(3) The specialist internship is a compulsory internship and is based on the Regulations for the Implementation of the Specialist Internship in the Bachelor's and Master's Degree Programmes at HTW Berlin in their currently valid edition and the Guidelines for the Content of Practical Training in accordance with Annex 7.

(4) The specialist internship is assessed on an undifferentiated basis. The programme is successfully completed when all the requirements of the Study and Examination Regulations for the Bachelor's degree programme Cyber Security and Business (see Annex 7) have been met.

§ 12 Module Examinations

(1) All modules, with the exception of the Specialist Internship module, are assessed in a differentiated manner.

(2) Successful completion of a module is evidenced by the student passing a standardised module examination. The type, form and scope of the module examinations are specified in the module descriptions for the Bachelor's degree programme Cyber Security and Business.

(3) In the event that the module examination is conducted as a combined examination in accordance with § 12, section 3 of the RStPO-Ba/Ma, the total number of points is 100, whereby the distribution of points must be shown in the module description.

(4) Passing the module examination is a requirement for gaining ECTS credits. The number of ECTS credits awarded for the respective modules is listed in Annexes 2 and 3.

(5) If the examination for an elective module has been passed, this module may not be replaced by another elective module. However, it is possible for the lecturer to issue a certificate of achievement for the additionally completed elective module.

(6) Admission to a module examination or other examination shall require registration for the corresponding module in accordance with the university regulations. It is mandatory to register for an examination in order to repeat a module examination that has been failed or not taken.

(7) Taking the examination for the B21 module ‘Project Sustainability in IT’ is only possible during the semester. To retake a module examination that has been failed or not taken, you must re-register for the module B21 ‘Project Sustainability in IT’.

§ 13 Final Examination: Bachelor’s Thesis

(1) The final examination consists of the Bachelor’s thesis and the final oral examination.

(2) Students who have successfully completed modules totalling at least 150 ECTS credits from the first to fifth semesters and have provided evidence of the specialist internship in the form of an internship contract may complete the Bachelor’s thesis. Candidates may also be admitted if they have not yet successfully completed modules totalling up to ten ECTS credits. The modules from the first three semesters must be completed.

(3) The Bachelor’s thesis must be registered with the faculty administration by the end of the 3rd week of the 6th semester. Permission to write the thesis, as granted by the Examination Board, must be issued by the end of the 9th week of the 6th semester.

(4) Upon registering or applying for permission to begin the process of final examination, the student shall offer a proposal for the topic and assessors of the final Bachelor’s Thesis. The Examination Board of the degree programme in question shall determine in writing the composition of the examination panel, the topic of the final thesis and the beginning and end of the completion period.

(5) The time required to complete the Bachelor’s thesis corresponds to 12 ECTS credits (360 working hours). The completion period for the Bachelor’s thesis is nine weeks (usually during weeks 10–19 of the sixth semester).

(6) The Bachelor’s thesis must be submitted to the faculty administration by the deadline in the required format, in accordance with § 26, section 7 of the RStPO-Ba/Ma in the currently valid edition.

(7) The Bachelor’s thesis must be written in English. The Bachelor’s thesis may be completed as a group thesis by two candidates. In each case, the contributions of each candidate must be definable and subject to individual assessment.

§ 14 Final Examination: Final Oral Examination

(1) To be eligible for the final oral examination, students must have achieved a grade of at least ‘sufficient’ for their Bachelor’s thesis and successfully completed all modules, totalling 177 ECTS credits, in the Bachelor’s degree programme Cyber Security and Business.

(2) The final examination (Bachelor’s thesis and final oral examination) is considered to have been passed when the Bachelor’s thesis and the final oral examination have been graded as at least ‘sufficient’ (4.0). The grading of the Bachelor’s thesis and the final oral examination is performed by means of a differentiated grade according to the mark scheme in § 17, section 1, column 2 of the

RStPO-Ba/Ma in the currently valid edition. The final examination grade X_2 is calculated using the formula below. The grade achieved is truncated after two decimal places.

$$X_2 = \frac{4}{5} X_{(21)} + \frac{1}{5} X_{(22)}$$

X_2 – final examination grade

$X_{(21)}$ – grade for the Bachelor's thesis

$X_{(22)}$ – grade for the final oral examination

(3) The final oral examination must focus predominantly on the topic of the Bachelor's thesis, including related and complementing fields of knowledge. The final oral examination should establish whether the student can independently verify the methodological procedures and the outcomes of Bachelor's thesis, possesses secure knowledge and understanding of the field addressed by the thesis and has mastered the requisite presentation and communication skills.

(4) In the event that the Bachelor's thesis was completed as a group project, the final oral examination should be organised as a joint examination.

§ 15 Module Groups and Module Grades on the Bachelor's Grade Transcript

(1) When calculating the final grade for the Bachelor's grade transcript, the modules named in section 2 are combined to form subject-specific module groups with their own designations. Unless stated otherwise, the overall grades of these module groups are determined by calculating the weighted mean of the individual module grades on the basis of the ECTS credits awarded for each module.

(2) The modules B12 - 'First Foreign Language' and B18 - 'First Foreign Language 2' constitute the module group Advanced Foreign Language English or Advanced Foreign Language French or Advanced Foreign Language Spanish or Advanced Foreign Language German (as a Foreign Language). The foreign language selected will be stated on the Bachelor's degree certificate.

(3) Sequence of modules/module groups on the Bachelor's grade transcript:

(a) Compulsory modules:

Programming

General Computer Science

Fundamentals of IT Security

Mathematics

IT Security in Law and Society

Scientific work

Statistics

Cloud IT

System Security

Web Applications/Software Architecture

Introduction to Business Administration

IT Networks

Cryptology

Databases

Social Engineering

Emergency Preparedness and Management

Mobile Devices

Network and System Security

Security Awareness

IoT Security

Digital Economy

IT Law and Data Protection

Norms, Standards & Certification

b) Specialisation: Forensics, or CI, or Distributed Ledger Technology (DLT), or subject-specific elective modules and projects

(Elective module 1)

(Elective module 2)

(Elective module 3)

(Elective module 4)

Project Sustainability in IT

c) Supplementary modules:

First foreign language: (Name of the selected foreign language)

Supplementary module or sub-modules

Advanced foreign language (if applicable): (Name of the selected foreign language), second foreign language if applicable: (Name of the selected foreign language)

(4) The grades for the modules

Mathematics

IT Security in Law and Society

Scientific Work

First foreign language

Supplementary module

are listed on the Bachelor's grade transcript, but are not included in the calculation of the final degree grade.

§ 16 Calculation of the Final Degree Grade

(1) The final degree grade is calculated using the overall grade (X), which is, in turn, derived from the weighted mean of the component grades (X_1, and X_2) according to the formula:

$$X=0{,}85X_1+0{,}15X_2$$

truncated after two decimal places and rounded to one decimal place. The component grades are:

a) the weighted mean module grade calculated from the credits for each module which is used to calculate the final grade (factor X_1); here the grade achieved is truncated after two decimal places, and

b) the final examination grade (factor X_2).

(2) The calculation of factor X1 for the final grade is performed via the calculation of a weighted mean of all modules based on their respective number of credits according to the formula

$$X_1 = \frac{\sum(F_i \cdot a_i)}{\sum a_i}.$$

Where:

- F_i: The individual module grades.
- a_i: The weighting factors (ECTS credits) of the individual modules.

(3) The weighting factors of the individual modules are listed in the following:

No.	Module Designation	Weighting Factor a_i
B1	Programming	5
B2	General Computer Science	5
B3	Fundamentals of IT Security	5
B7	Statistics	5
B8	Cloud IT	5
B9	System Security	5

B10	Web Applications/Software Architecture	5
B11	Introduction to Business Administration	5
B13	IT Networks	5
B14	Cryptology	5
B15	Databases	5
B16	Social Engineering	5
B17	Emergency Preparedness and Management	5
B19	Mobile Devices	5
B20	Network and System Security	5
B21	Project Sustainability in IT	5
B22	Elective module 1	5
B23	Elective module 2	5
B24	Security Awareness	5
B25	IoT Security	5
B26	Digital Economy	5
B27	IT Law and Data Protection	5
B28	Norms, Standards & Certification	5
B29	Elective module 3	5
B30	Elective module 4	5
	Total ECTS credits	**125**

§ 17 Graduation Documents

(1) Graduates shall receive graduation documents in accordance with § 31 of the Study and Examination Framework Regulations for Bachelor's and Master's Degree Programmes (RStPO-Ba/Ma) in the currently valid edition.

(2) The Bachelor's grade transcript indicates that the degree programme was completed in English. On the Bachelor's degree certificate in German, the module designations are listed in German; on the Bachelor's degree certificate in English, the module designations are listed in English. Conferral of the academic degree Bachelor of Science is certified via the Bachelor's degree certificate.

(3) Annexes 8 and 9 stipulate the details of the Diploma Supplement in German and English.

§ 18 Entry into Force/Publication

This regulation comes into force on the day after publication in HTW Berlin's Official Information Circular with effect from the 1st of October 2026.

Annex 1 Subject-Specific Higher Education Entrance Qualification According to § 11, Section 2 of the BerlHG

The following vocational training programmes are particularly suitable for enrolment in accordance with § 11, section 2 of the BerlHG:

- Assistant - Computer Science (General Computer Science)
- Assistant - Computer Science (Media Informatics)
- Assistant - Computer Science (Software Engineering)
- Assistant - Computer Science (Computer Engineering)
- Assistant - Computer Science (Business Informatics)
- Data Entry Specialist
- Specialist Consultant - Integrated Systems
- Specialist Consultant - Software Engineering
- IT Specialist
- IT Specialist - Application Development
- IT Specialist - Data and Process Analysis
- IT Specialist - Digital Networking
- IT Specialist - System Integration
- IT Administrator
- Information and Telecommunications Administrator
- Industrial Clerk
- Industrial Technologist
- IT Systems Electronics Engineer
- IT Systems Administrator
- Business Assistant - Business Informatics
- Business Assistant - Information Processing
- Digitisation Manager
- Security Technician (IT)
- IT System Management Administrator
- Business Assistant - Business Informatics
- Business Assistant - Information Processing
- Mathematical-Technical Assistant

- Mathematical-Technical Software Developer
- Technical Assistant - Electronics and Data Technology

The Examination Board decides on the comparability of the content of vocational training programmes with a designation other than those mentioned.

Annex 2 Programme Overview

1st semester

No.	Module Designation	Type	Cr	Lev	CP	RP	Form	WSH
B1	Programming	CM	5	1a	-	-	SSL PCE	3 2
B2	General Computer Science	CM	5	1a	-	-	SSL PCE	2 2
B3	Fundamentals of IT Security	CM	5	1a	-	-	SSL	4
B4	Mathematics	CM	5	1a	-	-	SSL PA	3 1
B5	IT Security in Law and Society	CM	5	1a	-	-	SSL	4
B6	Scientific Work	CM	5	1a	-	-	SSL PA	2 1
	Total ECTS credits for the semester		**30**					

2nd semester

No.	Module Designation	Type	Cr	Lev	CP	RP	Form	WSH
B7	Statistics	CM	5	1b	-	B4	SSL PCE	3 2
B8	Cloud IT	CM	5	1a	-	-	SSL PCE	2 2
B9	System Security	CM	5	1b	-	B3	SSL PCE	3 2
B10	Web Applications/Software Architecture	CM	5	1a	-	-	SSL PCE	2 2
B11	Introduction to Business Administration	CM	5	1a	-	-	SSL	4
B12	1st Foreign Language	EM	5	1a	-	-	PA	4
	Total ECTS credits for the semester		**30**					

3rd semester

No.	Module Designation	Type	Cr	Lev	CP	RP	Form	WSH
B13	IT Networks	CM	5	1a	-	-	SSL PCE	2 2
B14	Cryptology	CM	5	1b	-	B4	SSL PCE	2 1
B15	Databases	CM	5	1b	-	B10	SSL PCE	2 2
B16	Social Engineering	CM	5	1a	-	-	SSL PCE	2 2
B17	Emergency Preparedness and Management	CM	5	1a	-	-	SSL PCE	2 2
B18	Supplementary Elective Module	EM	5	1a	-	-	[1]	4
	Total ECTS credits for the semester		**30**					

4th semester (mobility semester)

No.	Module Designation	Type	Cr	Lev	CP	RP	Form	WSH
B19	Mobile Devices	CM	5	1a	-	-	SSL	2
B20	Network and System Security	CM	5	1b	-	B7	SSL PCE	2 2
B21	Project Sustainability in IT	EM	5	1b	-	B1, B11, B16, B17	PS	4
B22	Elective Module 1	EM	5	See Annex 3				4
B23	Elective Module 2	EM	5	See Annex 3				4
B24	Security Awareness	CM	5	1a	-	-	SSL	2
	Total ECTS credits for the semester		**30**					

[1] The course format depends on the specific module or sub-module on offer.

5th semester

No.	Module Designation	Type	Cr	Lev	CP	RP	Form	WSH
B25	IoT Security	CM	5	1b	-	B20	SSL PCE	2 2
B26	Digital Economy	CM	5	1a	-	-	SSL	4
B27	IT Law and Data Protection	CM	5	1b	-	B5	SSL	4
B28	Norms, Standards and Certification	CM	5	1b	-	B5	SSL	4
B29	Elective Module 3	CM	5	See Annex 3				4
B30	Elective Module 4	CM	5	See Annex 3				4
	Total ECTS credits for the semester		**30**					

6th semester

No.	Module Designation	Type	Cr	Lev	CP	RP	Form	WSH
B31	Specialist Internship Specialist Internship Seminar	CM	15	1b	See § 11		 PS[1]	 1
B32	Bachelor's Thesis	EM	12	1b	See § 13		BT	0
B33	Bachelor's Thesis Seminar and Final Oral Examination	CM	3	1b	See § 14		PS	1
	Total ECTS credits for the semester		**30**					
	Grand total ECTS credits for the degree programme		**180**					

[1] Takes place as a weekly virtual meeting with online support (e-learning).

Notes:

Form of teaching:

SSL	Seminar-Style Lecture	PCE	PC Exercise
AE	Accompanying Exercise	PS	(Project) Seminar
PE	Practical Exercise	BT	Bachelor's Thesis

Type of module:

CM	Compulsory Module	EM	Elective Module

General:

Cr	ECTS credits	WSH	Weekly Study Hours

RP Recommended Prerequisite (modules for which the completion of previous module examinations is recommended)

CP Compulsory Prerequisite (modules for which the completion of previous module examinations is required)

Lev Level (1a = prerequisite-free modules/1b = modules with prerequisites)

Explanatory notes:

One ECTS credit equates to student learning time (workload) of 30 hours (60 minutes). The workload of the Bachelor's thesis is 12x30 hours = 360 hours. The maximum completion time is nine weeks, with the result that the final oral examination may be conducted at the end of the semester if the Bachelor's thesis is submitted on time.

Annex 3 Elective Modules

Options for Elective Modules 1 to 4

Four modules totalling 20 ECTS credits can be selected from the modules offered in the 4th and 5th semesters. Students who have successfully completed modules totalling 15 ECTS credits from a specialisation (Forensics, CI or DLT) will have their chosen specialisation stated on their transcript. Otherwise, the modules selected will be listed under 'subject-specific elective modules' on the transcript. The assignment of modules to the respective specialisations and the prerequisites for the same are shown in the following table.

Module No.	Module Designation	Form	WSH	Lev	CP	RP	Forensics	CI	DLT	Comprehensive[1]
B110	Forensics in Operating and Application Systems	PCE	4	1b	-	B9	X			
B111	Analysis Methods for Forensic Data	PCE	4	1a	-	-	X			
B112	Forensic Psychology	PE	4	1a	-	-	X			
B113	Digital Investigation	PCE	4	1b	-	B16	X			
B114	Testing & Hacking	PCE	4	1b	-	B10				X
B115	Current Topics in Forensics	PE	4	1a	-	-	X			
B130	Critical Infrastructure Protection Objectives	PE	4	1b	-	B3		X		
B131	Security Operation (SOC)	PCE	4	1b	-	B10, B16		X		
B132	Handling Specific Risks	PE	4	1b	-	B17		X		
B134	Change Management (IT & HR)	PS	4	1b	-	B22				X
B135	Current Topics in CI	PE	4	1a	-	-		X		
B150	Fundamentals of Blockchain Technology/DLT	PCE	4	1b	-	B14			X	

[1] Modules in the 'Comprehensive' category are listed under the chosen specialisation. If no specialisation is chosen, the modules in the 'Comprehensive' category are listed under 'Subject-specific elective modules'.

B151	Token Economy, Cryptocurrencies and Digital Assets	PS	4	1a	-	-			X	
B152	Blockchain Business Development	PE	4	1b	-	B15			X	
B153	Blockchain Security	PCE	4	1b	-	B9			X	
B155	Current Topics in Blockchain Technology	PE	4	1b	-	B22			X	
B200	Emergency Management & Psychological Aspects	PE	4	1a	-	-				X

Annex 4 Supplementary Modules/Foreign Languages

The following options are available for the First Foreign Language module and the supplementary module:

Option 1 (in accordance with § 10, section 2, sentence 1, letter a) of the RStPO-Ba/Ma)

Option 1a:

No.	Module Designation	Type	Form	WSH	Cr	Lev	CP	RP
B12	Technical language English C1.1 Business (B) **or** Technical language French/Spanish B1.2 B **or** German[1] as a foreign language (at least at the level required for university admission)	EM	PA	4	**5**	1a	-	-
B18	Technical language English C1.2 B **or** Technical language French/Spanish B2.1 B **or** German as a foreign language (consolidating the level achieved in module B12)	EM	PA	4	**4**	1b	-	B12

Option 1b:

No.	Module Designation	Type	Form	WSH	Cr	Lev	CP	RP
B12	Technical language English C1.1 B **or** Technical language French/Spanish B1.2 B	EM	PA	4	**5**	1a	-	-

[1] applies only to students with a higher education entrance qualification in a language other than German

	or German[1] as a foreign language (at least at the level required for university admission)							
B18	Second Foreign Language:	EM	PA	4	**5**	1a	-	-

Option 2 (in accordance with § 10, section 2, sentence 1, letter b) of the RStPO-Ba/Ma)

No.	Module Designation	Type	Form	WSH	Cr	Lev	CP	RP
B12	Technical language English C1.1 B **or** Technical language French/Spanish B1.2 B **or** German[2] as a foreign language (at least at the level required for university admission)	EM	PA	4	**5**	1a	-	-
B18	Supplementary module (in accordance with § 10, section 2, sentence 1, letter b) of the RStPO-Ba/Ma)	EM	[3]	4	**5**	1a	-	-

Option 3 (in accordance with § 10, section 2, sentence 1, letter c) of the RStPO-Ba/Ma)

No.	Module Designation	Type	Form	WSH	Cr	Lev	CP	RP
B12	Technical language English C1.1 B **or** Technical language French/Spanish B1.2 B **or**	EM	PA	4	**5**	1a	-	-

[1] applies only to students with a higher education entrance qualification in a language other than German

[2] applies only to students with a higher education entrance qualification in a language other than German

[3] The format depends on the specific offers.

	German[1] as a foreign language (at least at the level required for university admission)							
B18	Supplementary module (in accordance with § 10, section 2, sentence 1, letter c)[2] of the RStPO-Ba/Ma)	EM	[3]	4	**5**	1a	-	-

[1] applies only to students with a higher education entrance qualification in a language other than German

[2] At the student's request, the Examination Board shall determine whether the chosen module may be recognised as a supplementary module.

[3] The format depends on the specific offers.

Annex 5 Module Overview

No.	Module Designation (German)	Module Designation (English)	Cr
B1	Programmierung	Programming	5
B2	Allgemeine Informatik	General Computer Science	5
B3	Grundlagen IT-Security	Fundamentals of IT Security	5
B4	Mathematik	Mathematics	5
B5	IT-Sicherheit in Recht und Gesellschaft	IT Security in Law and Society	5
B6	Wissenschaftliches Arbeiten	Scientific Work	5
B7	Statistik	Statistics	5
B8	Cloud IT	Cloud IT	5
B9	Sichere Systeme	System Security	5
B10	Webanwendungen/Software-Architektur	Web Applications/Software Architecture	5
B11	Einführung in die Betriebswirtschaftslehre	Introduction to Business Administration	5
B12	Erste Fremdsprache	First Foreign Language	5
B13	Netzwerke	IT Networks	5
B14	Kryptologie	Cryptology	5
B15	Datenbanken	Databases	5
B16	Social Engineering	Social Engineering	5
B17	Notfall-Vorsorge und Notfall-Management	Emergency Preparedness and Management	5
B18	AWE-Modul	Supplementary Elective Module	5
B19	Mobile Devices	Mobile Devices	5
B20	Netzwerk- und Systemsicherheit	Network and System Security	5
B21	Projekt Nachhaltigkeit in der IT	Project Sustainability in IT	5
B24	Security Awareness	Security Awareness	5
B25	IoT-Security	IoT Security	5
B26	Digitale Ökonomie	Digital Economy	5
B27	IT-Recht und Datenschutz	IT Law and Data Protection	5
B28	Normen, Standards & Zertifizierung	Norms, Standards and Certification	5
B31	Fachpraktikum	Specialist Internship	15

B32	Bachelorarbeit	Bachelor's Thesis	12
B33	Bachelorseminar und Abschlusskolloquium	Bachelor’s Thesis Seminar and Final Oral Examination	3
B110	Forensik in Betriebs- und Anwendungssystemen	Forensics in Operating and Application Systems	5
B111	Analysemethoden für forensische Daten	Analysis Methods for Forensic Data	5
B112	Forensik Psychologie	Forensic Psychology	5
B113	Digitale Ermittlungen	Digital Investigation	5
B114	Testing & Hacking	Testing and Hacking	5
B115	Aktuelle Themen der Forensik	Current Topics in Forensics	5
B130	Schutzziele KRITIS	Critical Infrastructure Protection Objectives	5
B131	Security Operation (SOC)	Security Operation (SOC)	5
B132	Umgang mit speziellen Risiken	Handling Specific Risks	5
B134	Change Management (IT & HR)	Change Management (IT & HR)	5
B135	Aktuelle Themen KRITIS	Current Topics in CI	5
B150	Einführung in die Blockchain-Technologie/DLT	Fundamentals of Blockchain Technology/DLT	5
B151	Token-Ökonomie, Kryptowährungen und digitale Vermögenswerte	Token Economy, Cryptocurrencies and Digital Assets	5
B152	Blockchain Business Development	Blockchain Business Development	5
B153	Blockchain Security	Blockchain Security	5
B155	Aktuelle Themen Blockchain-Technologie	Current Topics in Blockchain Technology	5
B200	Krisenmanagement & psychologische Aspekte	Emergency Management and Psychological Aspects	5

Annex 6 Learning Outcomes and Competences for each Module

1st semester

B1 Programming

Learning Outcomes and Competences
The students • are able to understand a problem algorithmically and transfer it into a programme; • create object-oriented programmes using standard classes; • understand the object-oriented class concept and learn how to modularise projects; • gain confidence in using an interpreter/compiler and a development environment; • learn to use relevant literature and documentation; • acquire the skills to learn independently, understand technological principles and find practical solutions to algorithmic problems; • are able to proceed in a conceptual and structured manner and develop systematic way of working; • expand their knowledge of object orientation by gaining confidence with the concept of object-orientated inheritance, abstract classes, interfaces and polymorphism; • acquire the ability to save and read data to and from files and to use dynamic data structures; • deepen their knowledge of programming in selected areas; • acquire the ability to master complex contexts through independent and systematic working methods, quickly familiarise themselves with unfamiliar topics and translate complex implementation problems into practical solutions.

B2 General Computer Science

Learning Outcomes and Competences
The students • are familiar with the basic principles of the structure of a computer; • are familiar with the number systems and character tables used in computer science and can assign them to the elementary data types of C; • are familiar with the most important addressing systems and basic principles of computer networks; • are familiar with the most important shell commands of a selected Linux shell, as well as regular expressions and environment variables; • are familiar with the key language elements for building shell scripts; • know the differences between interpreted and compiled programming languages; • are able to convert number systems into one another; • can handle MAC and IP addresses and execute simple network commands from the shell; • are able to operate a Linux operating system from the shell, for example, and write simple shell scripts; • can start interpreted programmes, for example Bash scripts or Python scripts; • can translate and run simple programmes in a compiled language (e.g. C programmes or Java programmes).

B3 Fundamentals of IT Security

Learning Outcomes and Competences
The students • understand the fundamental elements of IT systems, architectures, networks, IT infrastructures and operating systems with the following focal points: - fundamentals of information security and IT security, - IT security objectives, security interests and protection objectives, - threats, hazards and vulnerabilities, - roles, tasks and functions, - authentication and identities, - access control and authorisation concepts, - IT security management, concepts and procedures, - the importance of IT security for organisation, personnel and technology. • are familiar with the basic principles for creating IT security concepts; • acquire a necessary understanding of the system; • have the ability to understand IT security mechanisms for physical protection, authentication and access control and to recognise and implement key features.

B4 Mathematics

Learning Outcomes and Competences
The students • are able to abstract complex issues and describe them formally, logically correct and precisely in the language of mathematics; • are able to recognise and compare the complexity and feasibility of desired solutions to problems; • are able to calculate with real and complex numbers; • are able to determine the solutions of equations and inequalities; • are able to determine limits of sequences and series; • are able to calculate, derive and integrate rational, trigonometric, power, exponential and logarithmic functions; • are able to calculate with vectors and matrices; • are able to set up and solve systems of linear equations; • are able to set up simple mathematical models and draw logical conclusions from these; • are able to assess the accuracy of mathematical theorems by following proofs and prove simple theorems themselves.

B5 IT Security in Law and Society

Learning Outcomes and Competences
The students • gain an overview of the foundations of the rule of law (Germany and Europe) and the systematics of the general areas of law relevant to digitalisation (independent of contract type); • are familiar with fundamental concepts of general civil law, general law of obligations and other relevant areas of law such as intellectual property law, data protection law, the law of digital services and markets, private international law, IT security law and crypto-regulation; • are able to identify legal issues in the context of digitalisation after completing the module and develop initial solutions with the help of the dogmatics they have learned.

B6 Scientific Work

Learning Outcomes and Competences
The students • are proficient in methods of scientific work; • are able to independently obtain and evaluate data and information, select and obtain the relevant literature and cite sources correctly; • are familiar with the requirements for the content and formal design of written scientific papers and can present the content in a manner appropriate to the target audience and compose scientific texts; • are able to define, structure and plan complex tasks (time, resources, costs), allocate them to different team members, monitor progress, analyse risks and initiate countermeasures.

2nd semester

B7 Statistics

Learning Outcomes and Competences
The students acquire • a fundamental understanding of the procedure of descriptive statistics/contrast with inferential statistics; • an overview of data collection methods and important data sources in economic and social statistics; • knowledge of methods of descriptive univariate distribution analysis, correlation and regression as well as time series analysis; • knowledge of ratios/index numbers as a basis for the construction of value, price and quantity indices; • knowledge of the use of statistical software for data collection, data preparation and data analysis using the example of selected standard statistical software; • the ability to prepare and carry out computer-aided descriptive data analyses for selected problems using statistical software.

B8 Cloud IT

Learning Outcomes and Competences
The students • are familiar with the fundamental elements of cloud computing (particularly concepts, storage technologies, container (construction) and serverless computing); • are able to develop and deploy mobile applications independently; • are able to develop cloud deployment scenarios and operating scenarios and know how to implement them; • are able to set up a virtualisation environment; • are able to use SDN (Software Defined Networks) in the Could environment; • are able to create a simple cloud.

B9 System Security

Learning Outcomes and Competences
The students learn the essential features regarding • the fundamental concepts of IT system and network security; • historical and current attacks and vulnerabilities; • different types of attackers and attack patterns; • typical security risks; • the potential threats and security mechanisms on the various network layers of the ISO/OSI model (IPsec, TLS, 802.1x, RADIUS, Kerberos, OpenVPN, NATs and firewalls); • attack scenarios and defence options for client and server applications; • the risks and functionality of single sign-on systems; • the mode of operation and application of intrusion detection systems and honeypot systems. Furthermore, students are able to • determine adequate protection mechanisms for network communication; • configure firewall systems based on application requirements; • implement protection mechanisms for secure web communication based on TLS; • create and implement secure communication architectures; • recognise security risks in existing systems and isolate vulnerable applications from other applications; • understand and correctly categorise complex issues; • develop solutions; • apply methods of documentation and presentation in order to utilise these precisely for the target group in question.

B10 Web Applications/Software Architecture

Learning Outcomes and Competences
The students are familiar with • the typical features of web applications; • the fundamental elements of HTML, XHTML; • the fundamental elements of CSS; • the fundamental elements of JavaScript and JQuery; • client-server architecture; • the requirements for designing a web application from front-end to back-end. In addition, the students develop • a sound knowledge of methods and expertise in computer science and software development in order to develop new application and software systems, which they are able to modify and integrate within an existing application environment; • an understanding of and the ability to implement a customer's requirements with regard to the structure of a simple website; • an understanding of the architecture of modern web applications.

B11 Introduction to Business Administration

Learning Outcomes and Competences

The students understand
• fundamental economic models;
• economics with network theory;
• fundamental business management concepts;
  o strategy and organisation;
  o internal and external accounting;
  o controlling functions;
  o financing and investment;
  o marketing;
  o production.
In addition, the students are able to
• establish the connections between business and economic decisions;
• deduce the fundamental principles of business organisation, defining organisational concepts and situating the various functions of organisational structures within the broader context of cyber security and business;
• apply theoretical principles to practical examples.

3rd semester

B13 IT Networks

Learning Outcomes and Competences
The students • acquire a general understanding of how network systems work; • are familiar with the current network protocols and can assess the network situation in order to ensure the desired IT security level of a company / organisation; • are familiar with how security solutions work and develop an understanding of their use in operation and interaction; • are able to implement and use some of these solutions themselves. They can therefore • build and analyse networks; • configure routers and switches; • analyse network traffic; • assess the limitations of network technologies; • develop network applications.

B14 Cryptology

Learning Outcomes and Competences
The students • are familiar with the cryptological and cryptographic procedures and concepts presented as well as the associated methods; • are able to apply the methods considered and weigh them up against each other; • are able to perform simple safety analyses; • are able to penetrate the field of cryptology mathematically and to express the methods presented logically correctly and precisely in the language of mathematics; • are able to implement the most important procedures themselves. This includes • classic methods of cryptography; • symmetric procedures (DES, AES); • cryptographically secure random number generators; • hashing; • prime numbers and prime number tests; • Chinese remainder theorem; • asymmetric cryptography; • RSA; • digital certificates and certification authorities; • Diffie-Hellman; • elliptic curves and ECDH-RSA; • Blockchain and digital currencies; • methods of cryptanalysis.

B15 Databases

Learning Outcomes and Competences
The students • are able to translate the information requirements of comprehensive business processes into formal data models at a high level of abstraction and to implement these relationally; • are able to analyse relational databases using complex SQL queries; • are able to develop application programmes with access to database systems and create stored procedures; • familiarise themselves with architectural patterns for implementing the persistence layer of applications and gain an understanding of the structure of database systems; • receive an overview of performance-enhancing measures, data backup and rights management as well as a fundamental understanding of transactions.

B16 Social Engineering

Learning Outcomes and Competences
The students • understand social engineering fundamentals, and are, in particular, familiar with the most common types of attack and the necessary protection systems; • are able to analyse and assess attack vectors and optimise the quality of existing defence measures; • realise the limitations of purely technological measures; • learn tools and methods used by hackers to exploit human characteristics such as helpfulness, trust, fear or respect for authority in order to skilfully manipulate those affected; • know the possibilities of OSINT (Open Source Intelligence) for data acquisition and • are familiar with the extraction of relevant data from social networks, websites, media and other open sources; • are able to identify and implement solutions to classic problems after completing the module.

B17 Emergency Preparedness and Management

Learning Outcomes and Competences
The students • have a fundamental understanding of the processes involved in emergency situations: event - emergency - crisis; • are able to draw up an emergency management plan including the necessary resources; • are able to deploy immediate measures via the alarm system; • are able to create business continuation plans; • are able to write emergency manuals and emergency exercise plans; • are able to set up and maintain the necessary documentation.

4th semester

B19 Mobile Devices

Learning Outcomes and Competences
The students • are familiar with the features of mobile devices, networks and protocols; • are able to develop and test mobile systems according to given or self-created specifications; • are familiar with current architectures, APIs and deployment options for mobile applications (e.g. Android, IOS) and can provide mobile systems for the end user; • can apply their knowledge of cloud IT and derive knowledge of the relevant cloud architectures and the corresponding software solutions for cloud deployment scenarios; • are able to understand deployment scenarios for cloud applications and develop these accordingly; • are familiar with the special requirements for mobile applications and systems as well as the special requirements for cloud services from both the customer and provider perspective; • acquire a sound knowledge of methods and expertise in computer science and software development in order to develop and modify operational application systems and integrate these within an existing application environment; • are able to recognise and compare the complexity, feasibility, safety and degree of innovation of targeted problem solutions; • are able to recognise trends in the development of modern information technologies in relation to a specific application requirement and derive the necessary conclusions from the same.

B20 Network and System Security

Learning Outcomes and Competences
The students • are able to apply a basic understanding of cryptology (see Module B14) to cryptographic protocols and analyse them in terms of security objectives. • have a thorough understanding of modern cryptographic network protocols and are able to understand and reconstruct attacks on them. • are able to read and interpret the specifications of complex protocols in order to select appropriate configurations and algorithms for a given security level. • are able to abstract complex networks and systems in order to carry out a security analysis. • apply the basic strategies and countermeasures for securing networks and systems independently. The students are able to • select appropriate protocols, parameters and algorithms in order to achieve defined security objectives. • systematically analyse networks and systems with regard to security objectives. • use their knowledge of attack techniques to identify potential attack vectors. • select appropriate countermeasures to enhance the security of networks and systems.

B21 Project Sustainability in IT

Learning Outcomes and Competences
The students are able to • analyse the environmental impact of digital technologies and explain the energy and resource consumption of IT systems in the context of sustainable development; • take sustainability requirements into account when designing digital systems and to incorporate the relevant criteria as early as the planning phase of an IT project; • design and evaluate software architectures from a sustainability perspective, particularly with regard to energy efficiency, data volume, system complexity and scalability; • apply methods and tools for measuring and analysing software resource consumption, for example in terms of processing power, memory requirements, network usage or energy consumption; • implement energy-efficient and resource-conserving strategies, for example through optimised algorithms, efficient data processing or reduced data transmission; • analyse and optimise digital applications with regard to their contribution to sustainability by systematically evaluating technical solutions and identifying areas for improvement; • reflect on sustainability issues within interdisciplinary project contexts and to justify technical decisions by taking into account environmental, economic and social criteria; • document and present the results of a sustainability-focused IT project in a structured manner, including architectural decisions, resource analyses and optimisation measures.

B24 Security Awareness

Learning Outcomes and Competences
The students • comprehend that technical and organisational measures for initiating, maintaining and increasing IT/information security are important, but cannot establish complete protection if the human factor is neglected in the security chain; • are able to classify information security against the background of the 'human factor' and its relevance to labour law and the corresponding regulations; • understand how organisational rules and regulations work as structures that guide action; • can clearly identify the limits of regulations – both against the background of the regulations themselves and in the context of typical methods of attack (vishing, phishing, social engineering), as well as in terms of behaviour that cannot be regulated in methods of attack that are still unknown today (“unknown unknowns”); • recognise the need for comprehensive awareness-raising as a building block of company-wide information security; • learn the principles of effective communication and their influence on the effectiveness of rules and regulations in organisations; • become familiar with a set of generic awareness-raising measures and link these contextually with the principles of effective communication in order to create effective and specific awareness-raising measures, thereby enabling them to localise the complexity of 'sensitisation' using practical examples. • learn how successful awareness campaigns work and are able to orchestrate effective awareness communication and other awareness-building measures to create a targeted and effective awareness campaign; • learn which methods can be used to make awareness measurable and where the limits of the measurability of awareness currently lie.

5th semester

B25 IoT Security

Learning Outcomes and Competences
The students • learn about current security topics in connection with the IoT and common security architectures; • explore common cross-industry IoT use cases for connected vehicles, microgrids and enterprise drone systems; • are able to identify threats, vulnerabilities and risks; • learn about common IoT components and technologies to protect their systems and devices; • are able to implement the integration of data protection controls into the new IoT system designs; • learn how to deal with a real threat scenario for IoT systems and identify the highest priority risks; • analyse the data protection regulations and standards that apply to securing IoT systems and the confidentiality of stakeholder information; • address the challenges of privacy protection and remedial measures for the IoT in order to be able to propose adequate solutions.

B26 Digital Economy

Learning Outcomes and Competences
The students • learn the key features of digital markets and the ways in which these contrast with traditional, analogue markets; • are able to assess the fundamental determinants and challenges of the Internet economy; • are able to outline the typical challenges of a 'digital' company, e.g. in relation to e-business, e-commerce and e-marketing; • are familiar with information technology fundamentals for the development of e-business applications and shop systems and the differences in the area of business models for e-commerce; • understand the success factors of online marketing, social shopping, m-commerce, B2B auctions and payment systems as well as the platform economy.

B27 IT Law and Data Protection

Learning Outcomes and Competences
The students are familiar with the essential legal principles of IT security and are able to apply these. Key legal sources include the NIS Directive, the BSI Act, the Cybersecurity Regulation and the General Data Protection Regulation (Art. 32). Specifically, they are proficient in • the requirements for IT security management of critical infrastructures, digital services and companies in the special public interest; • the tasks, powers and services of the Federal Office for Information Security, in particular with regard to companies; • the security requirements for IT products, product certification, IT security labelling and special requirements for critical core components; • the special requirements of the GDPR for IT security when handling personal data (Art. 32); • tasks and powers of the data protection supervisory authority; • cooperation between the state and business in IT security; • sectoral legislation; In addition to these core issues, other legal issues relevant to IT security are also covered, in particular • responsibility of the company management; • contractual and tort law requirements for the IT security of products, update obligations; • the impact of industrial property rights on IT security; • criminal liability for IT security breaches; • conflicting objectives between IT security protection and attacks on IT security (hacker tools, vulnerability disclosure).

B28 Norms, Standards and Certification

Learning Outcomes and Competences
The students • are familiar with the key norms, standards and committees; • can adequately accompany a certification process; • are familiar with the legal regulations of German jurisdiction as well as the Cybersecurity Ordinance, BSI Act, Basel III + IV; SOX, GDPR; • are familiar with standards featuring IT security aspects such as COBIT (control objectives), ITIL (process library) IDW PS 300 (audit); • are familiar with the ISO standards for security measures and monitoring (ISO/IEC 18028 [Network], ISO/IEC TR 18044 [Security Incidents], ISO/IEC 18043 [Selection of an IDS], ISO/IEC TR 15947 [Guidelines for IDS], ISO/IEC 15816 [Access Control].

6th semester

B31 Specialist Internship

Learning Outcomes and Competences
The students • are familiar with the areas of application and application requirements of Cyber Security and Business in practice; • are familiar with practical collaboration in company projects; The students • are proficient in scientific working methods; • are able to independently obtain and evaluate data and information, select and obtain the relevant literature and cite sources correctly; • are familiar with the requirements for the content and formal design of written scientific papers and can present the content in a manner appropriate to the target audience and compose scientific texts; • are able to define, structure and plan complex tasks (time, resources, costs), allocate them to different team members, monitor progress, analyse risks and initiate countermeasures.

B32 Bachelor's Thesis

Learning Outcomes and Competences
The students have demonstrated • that they are able to successfully complete a specific task from their degree programme independently and use scientifically based theoretical and practical knowledge to solve a problem; • that they have the ability to work independently on a topic relevant to their studies and to write a professional paper.

B33 Bachelor's Thesis Seminar and Final Oral Examination

Learning outcomes and competences
The students • have the ability to write a scientific paper; • can present and justify their own approach and the results achieved.

Elective Modules

B110 Forensics in Operating and Application Systems

Learning Outcomes and Competences
The students • are able to identify relevant data sources and secure relevant data; • know how to restore deleted and changed data; • are familiar with and understand the IT forensic investigation procedure; • have an overview of IT forensics and the current state of the art; • can assess and evaluate the current challenges facing IT forensics; • are familiar with application scenarios and can utilise the possibilities of computer forensics; • are able to prepare, document and secure forensically recorded data as evidence that can be used in court. These include the fields of application • cybercrime; • IT attacks and their defence; • intrusion detection systems and suitable project documentation.

B111 Analysis Methods for Forensic Data

Learning Outcomes and Competences
The students • are able to carry out forensic data analyses in order to examine a company's data after incidents of economic crime (so-called fraud detection); • familiarise themselves with the analysis methods used to follow up data traces and to identify perpetrators and those involved in the offence; • are able to analyse underlying patterns of action and make appropriate recommendations for action; • familiarise themselves with and use the relevant testing software; • are able to use malware analysis and artificial intelligence to demonstrate how to detect digital threats, secure networks and solve criminal offences.

B112 Forensic Psychology

Learning Outcomes and Competences
The students • are familiar with the current tasks and developments in crisis management due to cyber attacks and the attendant psychological patterns; • learn, with the help of a simulation game, to put themselves in the position of both the attacker and the attacked in order to better assess the respective behaviours and to be able to incorporate appropriate solutions.

B113 Digital Investigation

Learning Outcomes and Competences
The students • are able to identify the most common fields of action and ways of preventing offences; • are familiar with the objectives and motivations of the perpetrators used to o collect access data or personal data; o encrypt files and data and extort ransom money, or o take control of the system; • learn to create preventive measures.

B114 Testing & Hacking

Learning Outcomes and Competences
The students • learn the tools and methods used to secure and analyse digital traces; • are familiar with the methods of penetration testing and can set up a test environment; • understand forensic principles when securing and analysing digital traces; • learn when and how to test which software in order to prevent damage from hackers, • can carry out a reproducible, technical security analysis of IT infrastructures. • can create a structured report on the results of a technical security analysis of IT infrastructure and present the results.

B115 Current Topics in Forensics

Learning Outcomes and Competences
The students • gain familiarity with current topics in the field of forensics, which relate, in particular, to security-related issues; • receive a deeper understanding of the fundamentals in order to better categorise current topics in their specific context.

B130 Critical Infrastructure Protection Objectives

Learning Outcomes and Competences
The students • can name the various sectors' protection objectives; • learn to define the requirements at a technical, procedural and organisational level; • are familiar with the BSI Act; • can determine the latest requirements on the basis of existing national and international standards.

B131 Security Operation (SOC)

Learning Outcomes and Competences
The students • are familiar with the special features of Security Operations Centres (SOC) and their role as a security control centre to ensure the protection of a company's or organisation's IT infrastructure; • learn that the SOC monitors and analyses all security-relevant systems such as company networks, servers, workstations and internet services; • learn that, among other things, the log files of the individual systems are collected, analysed and examined for anomalies and ascertain how this is to be carried out.

B132 Handling Specific Risks

Learning Outcomes and Competences
The students • are able to recognise and respond to risks and incidents; • understand the tools and necessary preparations required to minimise risk and reduce response time to incidents, crises and dangerous situations; • understand when, how and to whom concerns should be communicated while maintaining the appropriate confidentiality; • are familiar with the tools required to develop risk guidelines and, in particular, to identify IT-related risks. This also includes continuously evaluating and realigning the plan. • can also take psychological aspects into account; • learn the principles of effective communication and their influence on the effectiveness of rules and regulations in organisations.

B134 Change Management (IT & HR)

Learning Outcomes and Competences
The students • are familiar with the key methods of change management and, in particular, the special features of IT change management; • are able to explain important concepts in the areas of IT strategy, IT projects and IT operations from an overall business perspective; • are able to categorise current research approaches and developments on the basis of their sound knowledge of concepts and methods, develop them further independently and apply them accordingly; • are able to propose, assess and critically discuss change management in the field of IT.

B135 Current Topics in CI

Learning Outcomes and Competences
The students • gain familiarity of current topics in the field of critical infrastructure; • gain insights into current security-related issues in the CI sector; • receive a deeper understanding of the fundamentals in order to better categorise current topics in their specific context.

B150 Fundamentals of Blockchain Technology/DLT

Learning Outcomes and Competences
The students • have basic general knowledge and expertise as well as procedural knowledge in the field of distributed ledger technologies (distributed ledger techniques), particularly those pertaining to blockchain technology; • can classify and explain the various proposed solutions for distributed ledgers; • are able to summarise and explain the different methods of consensus building; • are able to specify the possible applications of different distributed ledger technologies and derive further possible applications; • are able to implement selected examples of distributed account books and consensus protocols; • are able to differentiate between existing and future proposals for blockchain technology and compare their respective advantages and disadvantages; • know how to check whether the use of blockchain technology makes sense for a given use case or whether conventional database solutions are sufficient.

B151 Token Economy, Cryptocurrencies and Digital Assets

Learning Outcomes and Competences
The students are able to • analyse different blockchain architectures (e.g. UTXO vs. account-based systems) in a comparative manner and evaluate them in terms of scalability, security and decentralisation; • understand complex ecosystems (e.g. DeFi protocols) as interconnected socio-technical systems; • systematically analyse and evaluate token models and crypto projects using appropriate criteria (e.g. tokenomics, governance, utility); • examine the interdependencies between cryptocurrency markets and traditional financial markets from both a quantitative and qualitative perspective; • model and assess risks (technical, economic, regulatory) from multiple perspectives. In addition, students are able to • design their own use cases for blockchain applications and assess them in terms of added value, feasibility and sustainability; • communicate with all stakeholders on a project-specific basis.

B152 Blockchain Business Development

Learning Outcomes and Competences
The students • familiarise themselves with the key features of blockchain technology and distributed ledger technology in the context of process optimisation and are able to identify these in a targeted manner according to requirements; • understand the different types of blockchain and are able to determine the appropriate architecture; • familiarise themselves with the common blockchain components and technologies to protect their processes, systems and data; • are able to implement the integration of data protection controls within the new blockchain system designs; • are familiar with the token economy and its characteristics; • can use this knowledge to decide which token model fits which business use case and design the corresponding framing; • are familiar with the current tasks and developments in the blockchain and token economy; • will be able to identify and implement solutions for the reorganisation of company processes with potential protection of critical data via a blockchain-based solution after completing the module; • develop both front-end and back-end solutions.

B153 Blockchain Security

Learning Outcomes and Competences
The students • learn about the fundamental elements of blockchain technology, including the various protocols and consensus mechanisms; • are able to distinguish between authentication and identification; • are familiar with the weak points of blockchain networks and can develop suitable countermeasures; • are able to distinguish between ‘Sybil Attacks’, ‘Phishing Attacks’, ‘Routing Attacks' and '51% Attacks”; • are able to develop a comprehensive security strategy for organisations that comprises, among other things, o identity and access management; o key management; o data protection; o secure communication; o security of smart contracts; o transaction confirmation. This includes • governance; • relevant regulatory requirements; • application of conventional security controls.

B155 Current Topics in Blockchain Technology

Learning Outcomes and Competences
The students • address current topics in the field of DLT / blockchain technology; • learn to assess the challenges posed by current topics (e.g. DeFi, NFTs, metaverse, etc.); • can categorise current topics (e.g. DeFi, NFTs, Metaverse etc.) in the context of the technology and its possible applications.

B200 Emergency Management & Psychological Aspects

Learning Outcomes and Competences
The students • are familiar with the current tasks and developments in crisis management in the event of cyber attacks; • are familiar with the fundamental elements of risk analysis and can apply these to specific cases and situations; • understand the importance of risk assessment and management-related fields of action in the context of cyber security in organisations; • are able to work in heterogeneous teams and fulfil leadership tasks; • understand ethical, legal, social, psychological and cultural aspects, requirements and challenges and are proficient in approaches to mitigate conflicts and dilemmas; • are familiar with the fundamental elements of the 'security economy' (aspects of risk management in the context of the functionality of economic processes and security risks); • are able to independently apply the risk assessment approaches and models of the crisis management cycle to case studies and scenarios; • have implementation expertise in terms of the identification of hazards related to critical infrastructure and the management of system-specific risks, taking existing security cultures into account.

Elective Modules/Foreign Languages

B12 First Foreign Language

English (technical language C1.1 B) **or** French/Spanish (technical language B1.2 B **) or** German[1] as a foreign language (at least at the level required for university admission)
Learning Outcomes and Competences
Technical language English C1.1 Business The students • perfect already acquired specialised language skills in the field of economics, • develop all language skills (listening, speaking, reading, writing) on this basis, • understand a wide range of demanding and extensive texts and also grasp implicit meanings, • can express themselves spontaneously and fluently without having to search for adequate expressions, • use the language flexibly and effectively in social, academic and professional contexts, • can express themselves in a clear, well-structured and detailed way on complex issues and use various means of linking texts appropriately. Technical language French/Spanish B1.2 Business The students • are introduced to the technical language of economics, • develop all language skills (listening, speaking, reading, writing) on the basis of general language skills already acquired, • understand the essential content of clear standardised information on familiar topics from the areas of work, school, study, etc., • acquire the ability to communicate in potential conversational situations in countries where the language is spoken, • can express themselves simply and coherently when speaking on familiar specialised topics or topics of personal interest, • can report on experiences and events and describe dreams, hopes and goals, • can give brief explanations and reasons for plans and opinions. German[2] as a foreign language Depending on their prior knowledge (which must, at least, satisfy the language requirements for university admission), students acquire general and/or specialised language skills in all areas of language proficiency (listening, speaking, reading and writing).

B18 First Foreign Language 2

Technical language English (C1.2 B) **or** technical language French/Spanish (B2.1 B) **or** German as a Foreign Language (building on the level achieved in module B12)
Learning Outcomes and Competences
Technical language English C1.2 Business The students • acquire a very high level of technical language competence in the field of economics, • develop all language skills (listening, speaking, reading, writing) on the basis of the First Foreign Language 1 module, • understand a wide range of demanding and extensive texts and also grasp implicit meanings, • can express themselves spontaneously, very fluently and precisely, • use the language flexibly and effectively in social, academic and professional contexts, • can express themselves in a clear, well-structured and detailed way on complex issues and use various means of linking texts appropriately, • learn to make finer nuances of meaning clear even in more complex situations. Technical language French/Spanish B2.1 Business The students • acquire further technical language skills in the field of economics, • develop all language skills (listening, speaking, reading, writing) on the basis of the First Foreign Language 1 module, • understand the main content of complex texts on concrete and abstract topics, • understand and present relevant topics in their own area of specialisation, • can hold appropriately fluent conversations, • can write clear and detailed texts on a range of specialised topics, • can present their own point of view on a specialised topic. German as a foreign language The students • acquire further general and/or specialised language skills, • develop all language proficiency skills (listening, speaking, reading, writing) on the basis of the First Foreign Language module.

[1] only applies to students with a higher education entrance qualification in a language other than German in accordance with § 9, section 4

[2] only applies to students with a higher education entrance qualification in a language other than German in accordance with § 9, section 4

B18 Second Foreign Language (not B12)

Learning Outcomes and Competences
Depending on their existing prior knowledge, students acquire general and/or specialised language skills in all linguistic areas (listening, speaking, reading, writing) according to the foreign language and level chosen by them from the range offered by the ZE FS (Central Foreign Languages Unit) (A1 to C1.2).

B18 Supplementary module

Learning Outcomes and Competences
The students • acquire cross-curricular or interdisciplinary skills, particularly social and communication skills ('soft skills'), and/or • gain a deeper understanding of the ways of thinking and approaches found in the humanities, communication studies, social sciences and cultural studies, and/or • will, upon completion of the module, be able to better understand other cultures and operate in different cultural contexts and/or • gain a deeper understanding of the potential and challenges of interdisciplinary academic collaboration.

Annex 7 Guidelines for the Specialist Internship in the Bachelor's Degree Programme Cyber Security and Business

§ 1 Training Areas and Content

(1) The specialist internship is a compulsory part of the degree programme. It can be completed in English or German in Germany or abroad. Students are familiarised with tasks in the field of business information security by working in a company for several weeks. They should apply their knowledge of methods and processes in practical situations to successfully solve typical cyber security and business tasks. They should also gain an insight into the technical, organisational, economic and social correlations between operational processes.

(2) Students can be employed in all fields of cyber security and business in companies from all sectors, in administration and in institutions. This includes, for example, tasks relating to critical infrastructure, forensic analysis of digital traces, IT security consulting and the use of distributed networks to secure data, data protection, etc. In cases of doubt, the internship coordinator decides whether a proposed activity can be assigned to this area of application.

§ 2 Duration and Implementation of the Specialist Internship

(1) The specialist internship usually takes place from the 24th week of the fifth semester until the end of the ninth week of the sixth semester; it may begin after the first examination period of the fifth semester upon request. It covers a period of at least twelve weeks, usually 37.5 hours per week. These 450 hours correspond to a student workload of 15 ECTS credit points (15•30 hours = 450 hours). In justified exceptional cases, a deviation of one working day is possible. This is decided by the internship coordinator for the Bachelor's degree programme Cyber Security and Business. A prerequisite is proof of 110 ECTS credits from modules taken in the first to fourth semesters of the degree programme.

(2) The course 'Specialist Internship Seminar' takes place as a regular virtual meeting with media support (e-learning).

§ 3 Supervision and Supporting Documents

(1) The internship coordinator of the Bachelor's degree programme Cyber Security and Business supports the students with regard to the preparation, implementation and evaluation of the internship.

(2) The following supporting documents are required for the successful completion of the specialist internship:

- an application for admission and approval of the internship before commencement of the same;

- an internship contract between the student and the internship company which must be accepted by the internship coordinator;
- a certificate from the internship company confirming the successful completion of the internship;
- a written practical report signed by the company where the internship was undertaken, detailing the time spent on the internship, the practical tasks involved and the respective activities required to complete the same.

(3) The internship is assessed by the internship coordinator on an undifferentiated basis.

Annex 8 Specific information on the Diploma Supplement in German

1. INFORMATION ON THE HOLDER OF THE QUALIFICATION

1.1 Surname(s) / 1.2 first name(s)

1.3 Date of birth (dd/mm/yyyy)

1.4 Matriculation number or student identification code (if available)

2. Information Regarding the Qualification

2.1 Title of qualification and (if applicable) degree awarded (in the original language)

Bachelor of Science, B.Sc.

2.2 Main fields of study for the qualification

Cyber Security and Business

with the specialisations:

forensics or

CI or

Distributed Ledger Technology

2.3 Name and status (type/body/organisation) of the awarding institution (in the original language)

Hochschule für Technik und Wirtschaft Berlin, Fachhochschule (FH) (Berlin University of Applied Sciences)

University of Applied Sciences / state

2.4 Name and status (type/funding body) of the institution (if not identical to 2.3) which implemented the programme (in the original language)

2.5 Language(s) of instruction/examination

English

3. INFORMATION ON THE LEVEL AND DURATION OF THE QUALIFICATION

3.1 Qualification level

First professional university degree from a scientific university (see sections 8.1 and 8.4.1) including a Bachelor's thesis

3.2 Official length of studies (regular study period) in credits and/or years

Regular study period:	6 semesters, 3 years
Workload:	5,400 hours
Credits (ECTS):	180 Cr
of which specialist internship	15 Cr
and Bachelor's thesis	12 Cr

3.3 Admission requirements

- General university/university of applied sciences entrance qualifications or higher education entrance qualification in accordance with § 11, sections 1 or 2 of the Berlin Higher Education Act (see section 8.7) and
- English proficiency at level C1 of the Common European Framework of Reference for Languages (CEFR)

4. Information on the Content of the Study Programme and Desired Learning Outcomes

4.1 Mode of study

Full-time, on-campus programme

4.2 Learning outcomes of the study programme

The Bachelor's programme equips students with the ability to design, develop and advance complex IT applications in the field of information security. The compulsory modules provide fundamental principles, methods, models and tools of computer science and information security, enabling students to conduct integrative analyses and to implement security-oriented information and communication systems. The programme also addresses the role of human factors in security-related processes.

In the specialisation phase, students acquire comprehensive knowledge of computer science, information security and business administration. They are qualified to plan, implement, operate, maintain and manage information-processing systems. In addition, they possess in-depth expertise in information security and IT forensics, take a proactive approach to securing existing systems, detect security-related attacks and are able to investigate security incidents.

The programme prepares students for professional roles that require an understanding of the technical, economic, social and ethical aspects of IT security. They develop the ability to work independently using scientific methods, apply academic knowledge in professional contexts, think critically and act responsibly within society.

Another key focus is on the ability to work in international contexts. This includes modules such as Digital Economy and Cloud IT, foreign language training, as well as an understanding of global standards, international IT security requirements, and the specific features of international software and network environments. Students reflect on the environmental, economic and social impacts of digital technologies and consider aspects of sustainability in the field of cyber security.

The skills acquired equip graduates for professional roles in business and IT security (security and safety), IT security in public administration, IT security and forensics, and IT security in the context of distributed ledger technologies.

Programme components:

Compulsory modules:	118 ECTS Cr
Optional elective modules (without a minimum requirement for foreign language study):	35 ECTS Cr
Minimum foreign language training:	5 ECTS Cr
Specialist internship:	15 ECTS Cr
Bachelor's thesis including final oral examination	15 ECTS Cr

4.3 Details of the degree programme, individually acquired credits and grades achieved

See the 'Bachelor's Degree Grade Transcript' for further details regarding areas of specialisation and the Bachelor's thesis topic, including grades.

4.4 Grading system and, if available, grade distribution table

4.5 Overall grade (in the original language)

– Final grade (not rounded off) -

Composition of final grade:

85 % module grades

15% final assessment (Bachelor's thesis and final oral examination)

5. Entitlement of Qualification

5.1 Access to further study

This degree entitles the holder to pursue a Master's degree; the respective Eligibility and Admission Regulations may stipulate additional requirements. (see section 8)

5.2 Access to regulated professions (if applicable)

n.a.

6. Additional Information

6.1 Additional information

The degree programme is accredited and bears the seal of the Accreditation Council (see: www.akkreditierungsrat.de).

6.2 Further information

Website: https://cyber-security-business.htw-berlin.de/

HTW Berlin: http://www.HTW-Berlin.de

Annex 9 Specific information on the Diploma Supplement in English

1. INFORMATION IDENTIFYING THE HOLDER OF THE QUALIFICATION
1.1 Surname(s)/1.2 first name(s)
1.3 Date of birth (dd/mm/yyyy)
1.4 Student identification number or code (if applicable)

2. INFORMATION IDENTIFYING THE QUALIFICATION
2.1 Name of qualification and (if applicable) title conferred (in the original language)
Bachelor of Science (B.Sc.)
2.2 Main field(s) of study for the qualification
Cyber Security and Business with the specialisations: forensics or CI or Distributed Ledger Technology
2.3 Name and status of awarding institution (in the original language)
Hochschule für Technik und Wirtschaft Berlin, Fachhochschule (FH) (Berlin University of Applied Sciences) University of Applied Sciences / state
2.4 Name and status (type/funding body) of the institution (if not identical to 2.3) which implemented the programme (in the original language)

2.5 Language(s) of instruction/examination

English

3. INFORMATION ON THE LEVEL AND DURATION OF THE QUALIFICATION

3.1 Qualification level

First professional university degree from a scientific university (see sections 8.1 and 8.4.1) including a Bachelor's thesis

3.2 Official length of studies (regular study period) in credits and/or years

Regular study period:	6 semesters, 3 years
Workload:	5,400 hours
Credits (ECTS):	180 Cr
of which specialist internship	15 Cr
and Bachelor's thesis	12 Cr

3.3 Admission requirements

- General university/university of applied sciences entrance qualifications or higher education entrance qualification in accordance with § 11, sections 1 or 2 of the Berlin Higher Education Act (see section 8.7) and
- English proficiency at level C1 of the Common European Framework of Reference for Languages (CEFR)

4. INFORMATION ON THE PROGRAMME COMPLETED AND THE RESULTS OBTAINED

4.1 Mode of study

Full-time, on-campus programme

4.2 Learning outcomes of the study programme

The Bachelor's programme equips students with the ability to design, develop and advance complex IT applications in the field of information security. The compulsory modules provide fundamental principles, methods, models and tools of computer science and information security, enabling students to conduct integrative analyses and to implement security-oriented information and communication systems. The programme also addresses the role of human factors in security-related processes.

In the specialisation phase, students acquire comprehensive knowledge of computer science, information security and business administration. They are qualified to plan, implement, operate, maintain and manage information-processing systems. In addition, they possess in-depth expertise in information security and IT forensics, take a proactive approach to securing existing systems, detect security-related attacks and are able to investigate security incidents.

The programme prepares students for professional roles that require an understanding of the technical, economic, social and ethical aspects of IT security. They develop the ability to work independently using scientific methods, apply academic knowledge in professional contexts, think critically and act responsibly within society.

Another key focus is on the ability to work in international contexts. This includes modules such as Digital Economy and Cloud IT, foreign language training, as well as an understanding of global standards, international IT security requirements, and the specific features of international software and network environments. Students reflect on the environmental, economic and social impacts of digital technologies and consider aspects of sustainability in the field of cyber security.

The skills acquired equip graduates for professional roles in business and IT security (security and safety), IT security in public administration, IT security and forensics, and IT security in the context of distributed ledger technologies.

Programme components:

Compulsory modules:	118 ECTS Cr
Optional elective modules (without a minimum requirement for foreign language study):	35 ECTS Cr
Minimum foreign language training:	5 ECTS Cr
Specialist internship:	15 ECTS Cr
Bachelor’s thesis including final oral examination	15 ECTS Cr

4.3 Details of the degree programme, individually acquired credits and grades achieved

See the ‘Bachelor’s Degree Grade Transcript’ for further details regarding areas of specialisation and the Bachelor’s thesis topic, including grades.

4.4 Grading scheme and notes on grading if available

4.5 Overall grade (in the original language)

- Final grade (not rounded off) -

Composition of final grade

85 % module grades

15% final assessment (Bachelor's thesis and final oral examination)

5. INFORMATION ON THE FUNCTION OF THE QUALIFICATION

5.1 Access to further study

This degree entitles the holder to pursue a Master's degree; the respective Eligibility and Admission Regulations may stipulate additional requirements. (see section 8)

5.2 Access to regulated professions (if applicable)

n.a.

6. ADDITIONAL INFORMATION

6.1 Additional information

The degree programme is accredited and bears the seal of the Accreditation Council (see: www.akkreditierungsrat.de).

6.2 Further information

Website: https://cyber-security-business.htw-berlin.de/

HTW Berlin website: http://www.HTW-Berlin.de