Curriculum – Deutsch

Lerneinheiten für Wissen, Fertigkeiten und Kompetenzen für Informationssicherheit und Datenschutz in KMU

Funded by the Erasmus+ Programme of the European Union

TeBelSi

Funded by the
Erasmus+ Programme
of the European Union

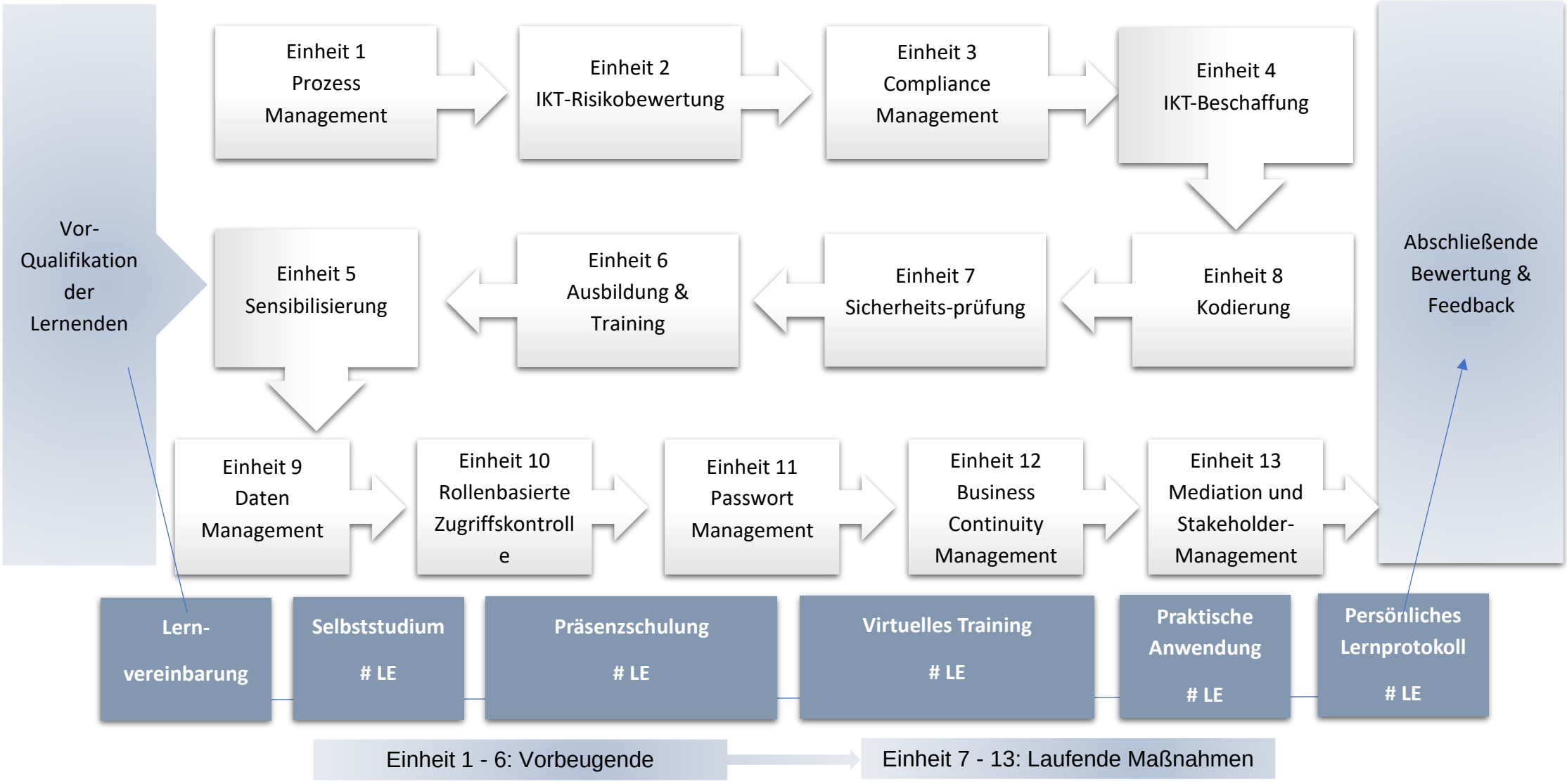
Dieses Dokument wurde im Rahmen des ERASMUS+ Project “Teilzertifizierung im Berufsfeld Informationssicherheit – TeBeiSi”, Projekt-Nr.: 2018-1-EN02-KA202-005218 erstellt.

Inhalt

Funded by the Erasmus+ Programme of the European Union

TeBeISi

TeBeISi Curriculum (based on ECVET criteria)



1.1 Lerneinheiten – Übersicht und Kurzbeschreibung

#	Lerneinheit	Kurzbeschreibung
LE1	**Prozess Management**	Analysieren Sie Geschäftsprozesse und erstellen Sie einen strategischen Bericht zum Thema Datenschutz und Informationssicherheit.
LE2	**IKT-Risikobewertung**	Verfolgen Sie Änderungen innerhalb und außerhalb des Unternehmens, die sich auf die Sicherheitsstrategie des Unternehmens auswirken, und erstellen Sie Berichte für die Mitarbeiter.
LE3	**Compliance Management**	Schreiben Sie Unternehmensrichtlinien, wie mit bestimmten Informationen und Daten umzugehen ist.
LE4	**IKT-Beschaffung**	Erarbeitung von Empfehlungen für zu beschaffende Artikel unter Berücksichtigung der Informationssicherheits- und Datenschutzanforderungen des Unternehmens.
LE5	**Sensibilisierung**	Durchführung von (Informations-)Aktivitäten zur Sensibilisierung der MitarbeiterInnen für Sicherheitsrisiken in ihrem Arbeitsalltag und zur Verbreitung des Bewusstseins in der Belegschaft.
LE6	**Ausbildung und Training**	Erstellen Sie Schulungspläne für das Unternehmen, um die MitarbeiterInnen regelmäßig in Bezug auf Informationssicherheit und Datenschutz ausbilden zu können.
LE7	**Sicherheitsprüfung**	Installieren Sie eine Firewall und Anti-Virus-Software. Führen Sie Updates durch und wenden Sie grundlegende Methoden an, um die Sicherheit der im Unternehmen eingesetzten Software zu testen und eine entsprechende Dokumentation zu erstellen.
LE8	**Kodierung**	Arbeiten Sie an der Absicherung von mobilen Geräten, Kommunikationskanälen und Datenspeichern über Passwörter oder andere Mittel der Authentifizierung.
LE9	**Daten Management**	Führen Sie routinemäßige Backups von Daten durch und wenden Sie Methoden des ordnungsgemäßen Verhaltens gemäß DSGVO auf die Datenverarbeitung im Unternehmen an.
LE10	**Rollenbasierte Zugriffskontrolle**	Richten Sie Administratorkonten ein und schränken Sie die Zugriffsrechte der MitarbeiterInnen entsprechend der definierten Sicherheitsstufen ein.
LE11	**Passwort Management**	Legen Sie Passwörter für den individuellen Zugriff der MitarbeiterInnen fest und sorgen Sie für eine sichere Speicherung und Wiederherstellung.
LE12	**Business Continuity Management**	Legen Sie Richtlinien und Verfahren für das Auftreten von möglichen Eventualitäten fest.
LE13	**Mediation & Stakeholder-Management**	Koordinieren Sie die Bedürfnisse von Führungskräften und MitarbeiterInnen des Unternehmens und versorgen Sie beide Parteien mit Informationen und Einblicken aus dem Unternehmen.

2 Detaillierte Beschreibung der Lerneinheiten (basierend auf ECVET)

2.1 LU1 – Prozess Management

Lerneinheit 1	Prozess Management
Allgemeine Beschreibung / Ausgang	**Analysieren Sie Geschäftsprozesse und erstellen Sie einen strategischen Bericht zum Thema Datenschutz und Informationssicherheit.**
Code-Nummer	LE 1
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen die Bedeutung einer strukturierten Prozessanalyse in einem Unternehmen zu verstehen. Sie sind in der Lage, Prozesse zu erkennen, die aufgrund ihrer Daten- und Informationssicherheitsgefährdung die Notwendigkeit einer weiteren Analyse hervorrufen. Die TeilnehmerInnen sind mit der Prozessdokumentation vertraut und sind in der Lage, Veränderungen im Arbeitsablauf zu überwachen. Sie sind in der Lage, eine Dokumentation zu erstellen, die die Formulierung von Handlungsempfehlungen ermöglicht.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - wie man die DSGVO-Richtlinien und gute Informationssicherheitspraktiken anwendet. - wie man Geschäftsprozesse identifiziert, dokumentiert, gestaltet, implementiert, steuert und optimiert. - wie man die Prozessdokumentation strategisch plant. - über Kommunikationstechniken und -kanäle. **Können** - Dokumentation mit Hilfe von EDV-Systemen realisieren. - die ursprüngliche Information zusammenfassen, ohne dass die ursprüngliche Nachricht verloren geht. - effektiv mit KollegInnen kommunizieren, um Arbeitsabläufe anzupassen. - angemessen auf die Aussagen anderer reagieren, z. B. konstruktive Kritik annehmen und aktiv zuhören, um die besten Lösungen zu finden. - finden Sie relevante rechtliche und technische Informationen und entsprechende Handlungsempfehlungen aus vertrauenswürdigen Quellen.

	Persönliche Kompetenz **Die TeilnehmerInnen sind in der Lage** - organisieren selbstständig den Dokumentationsprozess und arbeiten strukturiert und detailorientiert. - selbständig mit KollegInnen zu kommunizieren und sicher im Umgang zu sein. - die zur Aufgabe gehörende Verantwortung erkennen und sicher im Umgang mit anderen sein. -
Empfehlungen für Lernen & Lehren	Prozessdokumentation mit Hilfe von Beispielen aus der Praxis. Übungen zur Dokumentation im EDV-System in freier Form und mit Hilfe von Textbausteinen.
Literatur & weitere Ressourcen	Nguyen, B. T., Lee, G. M., Sun, K., & Guo, Y. (2019). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security,* 15, 1-13. EU-GDPR. (2019). *EU-GDPR-Portal*. [Online]. Verfügbar: https://eugdpr.org. Allgemeine Datenschutzverordnung (2018). Amtsblatt der Europäischen Union [Online]. Verfügbar: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:32016R0679. Gellert, R. (2015). Datenschutz als Risikoregulierung begreifen. *Zeitschrift für Internetrecht*, 18 (11), 3-15.

2.2 LU2 – IKT-Risikobewertung

Lerneinheit 2	IKT-Risikobewertung
Allgemeine Beschreibung / Ausgang	**Verfolgen Sie Änderungen innerhalb und außerhalb des Unternehmens, die sich auf die Sicherheitsstrategie des Unternehmens auswirken, und erstellen Sie Berichte für die MitarbeiterInnen.**
Code-Nummer	LE 2
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen, die Dynamik des technologischen Wandels und deren Einfluss auf die Unternehmensstrategie zur Risikominimierung zu verstehen. Sie sind in der Lage, über die Dringlichkeit der Reaktion auf diese Risiken zu entscheiden. Die TeilnehmerInnen sind in der Lage, technologische Entwicklungen innerhalb und außerhalb des Unternehmens zu verfolgen und Einschätzungen über die Risikoexposition des Unternehmens abzugeben.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - über die Bewertung der Risikoexposition der Firma und die Angemessenheit der aktuellen Maßnahmen zur Bewältigung der damit verbundenen Risiken. - wie man technologische Entwicklungen innerhalb und außerhalb der Firma sowie Veränderungen beim Personal überwacht. - wie man den Umfang und den Zweck der verarbeiteten personenbezogenen Daten bestimmt. **Können** - sich über technologische Entwicklungen zu informieren, indem sie einschlägige Nachrichtenquellen und Informationen von öffentlichen oder privaten Stellen aus der Praxis zu Rate ziehen. - Risiken trotz theoretischer Zurückhaltung der MitarbeiterInnen, Fehler oder Schwächen zu offenbaren, zu erkennen. - Handlungsempfehlungen auf Basis der gewonnenen Informationen geben. - Risiken in Bezug auf den Datenschutz zu bewerten und zu minimieren. - personenbezogene Datenspeicher/Verarbeitungsvorgänge in Organisationen zu identifizieren und deren Kontext zu bewerten. - Maßnahmen zu den auf Strategieebene festgelegten Zielen zu ergreifen, um Ressourcen und Mitarbeiter zu mobilisieren und die Zusammenarbeit zu stärken.

	Persönliche Kompetenz **Die TeilnehmerInnen sind in der Lage** - Belastbarkeit zeigen, wenn sie mit mangelnder Kooperationsbereitschaft von KollegInnen konfrontiert sind. - flexibel bleiben, um Lösungen zu finden und eine unterstützende Umgebung zu schaffen. - Aufgaben strategisch und organisiert ausführen. -
Empfehlungen für Lernen & Lehren	Prozessdokumentation mit Hilfe von Beispielen aus der Praxis. Übungen zur Dokumentation im EDV-System in freier Form und mit Hilfe von Textbausteinen.
Literatur & weitere Ressourcen	European Banking Authority (2019). Final Report: EBA Guidelines on ICT and security risk management [Online]. Verfügbar: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020. NZ Digital Government (2021). ICT Risk Management Guidance [Online]. Verfügbar: www.digital.govt.nz/dmsdocument/130-ict-risk-management-guidance/html. Commission de Surveillance du Secteur Financier (CSSF) (2020). ICT Risk [Online]. Verfügbar: www.cssf.lu/en/ict-risk/. Rothman, T. (2020). Valuations of Early-Stage Companies and Disruptive Technologies: How to Value Life Science, Cybersecurity and ICT Start-ups, and their Technologies. Berlin: Springer.

2.3 LU3 – Compliance Management

Lerneinheit 3	Compliance Management
Allgemeine Beschreibung / Ausgang	**Schreiben Sie Unternehmensrichtlinien, wie mit bestimmten Informationen und Daten umzugehen ist.**
Code-Nummer	LE 3
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen zu verstehen, wie wichtig die Kodifizierung von Verhaltensrichtlinien im Unternehmen ist, um den richtigen Umgang mit Daten und Informationen zu etablieren. Sie lernen, wie man Richtlinien festlegt, die bei den Mitarbeitern Compliance etablieren. Sie verstehen, wie wichtig es ist, sich auf vorhersehbare und unvorhersehbare Eventualitäten vorzubereiten und unternehmensweite Regeln festzulegen, wie man sich in kritischen Situationen verhält und welche Maßnahmen zu ergreifen sind.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - über den Bereich der DSGVO-Vorschriften und nationalen Rechtsdokumente, die die Informationssicherheit und den Datenschutz regeln. - über die Informationsarchitektur und die internen Kommunikationskanäle der Organisation - wie man Prozesse analysiert, abbildet und dokumentiert, die einen potenziellen Konflikt mit Compliance-Richtlinien verursachen könnten. - wie man Compliance-Richtlinien erstellt. - wie man Datenverarbeitungstechniken sammelt, verwaltet und bewertet. - wie man analytisch denkt, um Informationen zu verdichten, Lösungen zu entwickeln und Entscheidungen im Zusammenhang mit Compliance Management zu treffen. **Können** - die in Rechtsdokumenten beschriebenen Verfahren umzusetzen. - kritische Daten- und Informationseinheiten identifizieren, die einen besonderen Schutz oder eine besondere Behandlung erfordern. - die Prozesse im Zusammenhang mit dem Informationsfluss in der Organisation zu analysieren und abzubilden. - mögliche Risiken und Bedrohungen für die Informationssicherheit und den Datenschutz in den internen Prozessen der Organisation zu erkennen. - entwickeln Compliance-Management-bezogene Lösungen für praktische, betriebliche oder konzeptionelle Probleme in einem weiten Bereich der täglichen Arbeitsabläufe.

	- den Zweck der Compliance-Richtlinien zu verstehen und sie in Notfallsituationen zu aktualisieren. - analytische und kritische Denkfähigkeiten anwenden, um die Stärken und Schwächen potenzieller Lösungen für Probleme im Zusammenhang mit dem Compliance-Management zu identifizieren. - fassen die Informationen auf bequeme und sinnvolle Weise zusammen. **Persönliche Kompetenz** **Die TeilnehmerInnen sind in der Lage** - strukturiert und detailorientiert zu arbeiten. - die zu den Aufgaben gehörende Verantwortung erkennen und sicher im Umgang mit anderen sein. - Aufgaben selbständig erledigen und Lernbereitschaft zeigen. -
Empfehlungen für Lernen & Lehren	Prozessdokumentation mit Hilfe von Beispielen aus der Praxis. Übungen zur Dokumentation im EDV-System in freier Form und mit Hilfe von Textbausteinen.
Literatur & weitere Ressourcen	Agostinelli S., Maggi F.M., Marrella A., & Sapio F. (2019) Achieving GDPR Compliance of BPMN Process Models. In: Cappiello C., Ruiz M. (eds) Information Systems Engineering in Responsible Information Systems. CAiSE 2019. Lecture Notes in Business Information Processing, 350, 10-22. Springer, Cham. https://doi.org/10.1007/978-3-030-21297-1_2 Basin, D., Debois, S., & Hildebrandt, T. (2018). On purpose and by necessity: compliance under the GDPR. In Proceedings Financial Cryptography and Data Security, 18 [Online]. Verfügbar: https://pure.itu.dk/ws/files/84212312/On_Purpose_and_ny_Necessity.pdf. Besik, S. I., & Freytag, J. C. (2020). Managing Consent in Workflows under GDPR. In J. Manner, S. Haarmann, S. Kolb, O. Kopp (Eds.): 12th ZEUS Workshop, ZEUS 2020, Potsdam,Germany, 20-21 February 2020, (pp. 18-25). Blanco-Lainé, G., Sottet, J. S., & Dupuy-Chessa, S. (2019, November). Using an enterprise architecture model for GDPR compliance principles. In IFIP Working Conference on The Practice of Enterprise Modeling (pp. 199-214). Springer, Cham. EU-GDPR. (2019). EU-GDPR-Portal. [Online]. Verfügbar: https://eugdpr.org. Kammüller, F., Ogunyanwo, O.O., & Probst, C.W. (2019). Designing data protection for GDPR compliance into IoT healthcare systems. Computer Science. arXiv:1901.02426.

	Torre, D., Soltana, G., Sabetzadeh, M., Briand, L. C., Auffinger, Y., & Goes, P. (2019). Der Einsatz von Modellen zur Überprüfung der Einhaltung der GDPR: An Experience Report. In 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS), Munich, Germany, 2019, (pp. 1-11). doi: 10.1109/MODELS.2019.00-20. Wichmann, J., Sandkuhl, K., Shilov, N., Smirnov, A., Timm, F., & Wißotzki, M. (2020). Enterprise Architecture Frameworks als Unterstützung bei der Umsetzung von Regulierungen: Ansatz und Erfahrungen aus der GDPR. Complex Systems Informatics and Modeling Quarterly, (24), 31-48.

2.4 LU4 – IKT-Beschaffung

Lerneinheit 4	IKT-Beschaffung
Allgemeine Beschreibung / Ausgang	**Erarbeitung von Empfehlungen für zu beschaffende Artikel unter Berücksichtigung der Informationssicherheits- und Datenschutzanforderungen des Unternehmens.**
Code-Nummer	LE 4
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen, die Bedeutung der Beschaffung zur Unterstützung der Umsetzung von Informationssicherheit und Datenschutz zu verstehen. Sie lernen, die eigene Expertise im Beschaffungsprozess des Unternehmens zu positionieren. Die TeilnehmerInnen sind in der Lage, Einfluss auf die Beschaffung neuer Technik und Maschinen zu nehmen und die Angemessenheit und Verwendbarkeit im Hinblick auf die Datenschutz- und Informationssicherheitsrichtlinien des Unternehmens zu bewerten.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - über Sicherheits- und Spezifikationsanforderungen der Firma an neue Geräte. - über die Spezifikationen der vorhandenen Hardware und die Dringlichkeit, diese mit neuer Technologie zu verändern. - über die Täuschung von DienstleisterInnen und Geräten zu DSGVO-Verstößen. **Können** - effektiv mit anderen zu kommunizieren. - eine kurze Präsentation (Bericht/Ablauf/Prozess/Strategie) zur Bewertung von Technologie oder Maschinen, die angeschafft werden müssen, vorbereiten und präsentieren. - Informationen von verschiedenen MitarbeiterInnen / Abteilungen über ihre Bedürfnisse zu übertragen und dann die Empfehlung zum Kauf zu geben. - umfassende Informationen über gekaufte Technik/Maschinen zu sammeln. - relevante rechtliche und technische Informationen zu finden und Entscheidungen auf Basis dieser Recherche zu treffen. - Maßnahmen zu den auf strategischer Ebene definierten Zielen und Verfahren zu ergreifen, um Ressourcen zu mobilisieren und die festgelegten Strategien zu verfolgen.

	- Ressourcen unter Budget- und Zeitvorgaben zu planen und zu verwalten und die gesetzten Ziele zu erreichen, wobei die Überwachung des Projektfortschritts und Qualitätskontrollen genutzt werden. **Persönliche Kompetenz** **Die TeilnehmerInnen sind in der Lage** - sich über bestehende Marktlösungen für das Problem der Firma informieren. - widmen sich den Details (rechtlich und technisch). - Vertrauen und Verantwortung in der Kommunikation mit Stakeholdern zeigen.
Empfehlungen für Lernen & Lehren	Prozessdokumentation mit Hilfe von Beispielen aus der Praxis. Übungen zur Dokumentation im EDV-System in freier Form und mit Hilfe von Textbausteinen.
Literatur & weitere Ressourcen	Australische Regierung: Digital Transformation Agency (2021). ICT procurement [Online]. Verfügbar: www.dta.gov.au/help-and-advice/ict-procurement. Moses, M. (2019). Beschaffungsprozess und IKT. Zerite Network [Online]. Verfügbar: http://zeritenetwork.com/procurement-process-and-ict/. Europäische Kommission (2016). Best Practices for ICT procurement based on standards in order to promote efficiency and reduce lock-in: 2-year project completed [Online]. Verfügbar: ec.europa.eu/digital-single-market/de/news/. Dovgalenko, S. (2020). The Technology Procurement Handbook: A Practical Guide to Digital Buying. London: Kogan Page.

2.5 LU5 – Sensibilisierung

Lerneinheit 5	Sensibilisierung
Allgemeine Beschreibung / Ausgang	**Durchführung von (Informations-)Aktivitäten zur Sensibilisierung der Mitarbeiter für Sicherheitsrisiken in ihrem Arbeitsalltag und zur Verbreitung des Bewusstseins in der Belegschaft.**
Code-Nummer	LE 5
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Der TeilnehmerInnen lernt zu verstehen, wie wichtig die Sensibilisierung von MitarbeiterInnen und VorständInnen für die Belange des Datenschutzes und der Informationssicherheit ist. Sie lernen, das Bewusstsein für gängige Bedrohungen zu schärfen und Kapazitäten bei der Belegschaft aufzubauen, um wahrscheinliche Bedrohungen im Arbeitsalltag zu erkennen. Die TeilnehmerInnen werden in die Lage versetzt, Analysen über den Bewusstseinsstand im Unternehmen durchzuführen und entsprechende Sensibilisierungsmaßnahmen umzusetzen.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - über grundlegende Richtlinien der DSGVO. - wie man mit potenziellen Prozessen und MitarbeiterInnen umgeht, die anfällig für Angriffe oder den Verlust von sensiblen Informationen und Daten sind. - wie Revisionsmaßnahmen durchgeführt werden können. - über Kommunikationstechniken und -kanäle. - wie man Veränderungsstrategien umsetzt. **Können** - die entsprechende Rechtsquelle zu finden. - mit anderen im weitesten Sinne des Wortes zusammenarbeiten, um den Bedarf an Veränderung zu erkennen, zu inspirieren und anzuleiten und bei der Umsetzung zu helfen. - effektiv mit anderen kommunizieren, indem sie nicht nur die Art der Nachricht, sondern auch deren Umfang und Bedeutung für die Umstände wählen. **Persönliche Kompetenz** **Die TeilnehmerInnen sind in der Lage**

	- sich an veränderte Bedingungen und Umstände anzupassen, indem sie organisiert arbeiten und einen Abstand einhalten, der eine angemessene Selbsteinschätzung ermöglicht. - ein Beispiel für andere MitarbeiterInnen zu sein, die ihrem ethischen Verhaltenskodex folgen und Verantwortung zeigen.
Empfehlungen für Lernen & Lehren	Kombinieren Sie theoretisches Wissen und Vorgehen mit praktischen Beispielen wie z.B. Bauchcheck-Maßnahmen und Inszenierung von Ereignissen: - Gefälschte USBs - Instanzen des Human Engineering - Versenden von gefälschten e-Mails Interaktive Lehrmethoden anwenden (z. B. Gruppenarbeit, Diskussionen, Fallanalysen, Simulationsrollenspiele usw.)
Literatur & weitere Ressourcen	IT Governance Privacy Team (2020). EU General Data Protection Regulation (GDPR) - An implementation and compliance guide (4th ed.). Clarke, N., Furnell, S. (2020). Human Aspects of Information Security & Assurance (14th ed.). Plymouth: Centre for Security, Communication & Network Research. i-scoop (o.J.). GDPR-Bewusstsein: eine Frage von Menschen, Kultur, Führung und Handeln jetzt [Online]. Verfügbar: https://www.i-scoop.eu/gdpr/gdpr-awareness/. Kefron - The Information Management People (o.J.). Why Maximizing Staff Awareness Is The Key To A Smooth GDPR Transition [Online]. Verfügbar: https://www.kefron.com/blog/why-maximizing-staff-awareness-is-the-key-to-a-smooth-gdpr-transition/. European Union Agency for Cybersecurity (2017). Handbook on Security of Personal Data Processing [Online]. Verfügbar: www.enisa.europa.eu General Data Protection Regulation (2021). Vollständiger Leitfaden zur Einhaltung der GDPR [Online]. Verfügbar: https://gdpr.eu/

2.6 LU6 – Ausbildung und Training

Lerneinheit 6	Ausbildung und Training
Allgemeine Beschreibung / Ausgang	**Erstellen Sie Schulungspläne für das Unternehmen, um die MitarbeiterInnen regelmäßig in Bezug auf Informationssicherheit und Datenschutz schulen zu können.**
Code-Nummer	LE 6
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen, die Bedeutung der Aufklärung in Bezug auf die Anforderungen des Datenschutzes und der Informationssicherheit zu verstehen. Sie lernen, sowohl sich selbst als auch die MitarbeiterInnen des Unternehmens zu schulen. Die TeilnehmerInnen sind in der Lage, verlässliche Quellen zu konsultieren und den Schulungsbedarf nach Rücksprache oder in Interaktion mit den MitarbeiterInnen abzuleiten. Die TeilnehmerInnen lernen, Schulungsunterlagen vorzubereiten und die KollegInnen zu schulen, um entsprechende Arbeitsabläufe in ihre tägliche Arbeit einzubauen.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - wo Sie nationale Rechtsdokumente finden, die die Informations-sicherheit und den Datenschutz regeln (Grundlagen der DSGVO). - wie man Schulungsmaterial vorbereitet und wie man Schulungen durchführt, um angemessene Arbeitsroutinen einzubauen. - wie Sie einzelne MitarbeiterInnen betreuen. **Können** - die MitarbeiterInnen in die praktische Anwendung nationaler Rechtsdokumente im Bereich der Informationssicherheit und des Datenschutzes nach den Richtlinien der DSGVOeinführen. - Mitarbeiter durch aktive Bewusstseinsbildung von der Wichtigkeit der kontinuierlichen Weiterbildung in beiden Bereichen zu überzeugen. - Mentor und Unterstützer einzelner MitarbeiterInnen in Bezug auf identifizierten Schulungsbedarf. - Lösungen für praktische, betriebliche oder konzeptionelle Probleme zu entwickeln, die bei der Ausführung von Arbeiten in einem breiten Spektrum von Kontexten auftreten. **Persönliche Kompetenz** **Die TeilnehmerInnen sind in der Lage**

	- selbstständig Schulungen im Unternehmen strukturiert und bedarfsorientiert zu organisieren. - selbstbewusst mit KollegInnen und der Geschäftsleitung zu kommunizieren, indem sie sicher im Umgang miteinander sind. - die zur Aufgabe gehörende Verantwortung erkennen und die Mitarbeiter zum Lernen motivieren.
Empfehlungen für Lernen & Lehren	Dokumentation von Informationssicherheits- und Datenschutzproblemen, die im Tagesgeschäft auftreten, um entsprechende Schulungsmaßnahmen zu planen und durchzuführen.
Literatur & weitere Ressourcen	Pipkin, D. (2000). Informationssicherheit: Protecting the global enterprise. New York: Hewlett-Packard Company. Da Veiga, A., Martins, N. (2015). Verbesserung der Informationssicherheitskultur durch Überwachungs- und Implementierungsmaßnahmen, veranschaulicht durch eine Fallstudie. Computers & Security, (49), 162-176. doi: 10.1016/j.cose.2014.12.006. Peacock, M., Steward, E. B., & Belcourt, M. (2019). Understanding Human Resources Management. Nelson: Nelson College Indigenous. Ryan, L. (2010). Corporate Education: A Practical Guide to Effective Corporate Learning. Salisbury: Griffin Press. Osborne, B. (2020). 10 Vorteile von Security Awareness Training [Online]. Verfügbar: https://resources.infosecinstitute.com/topic/10-benefits-of-security-awareness-training/. GDPR informer (2017). Datenschutzschulung: 10 Tipps für Ihre Mitarbeiter [Online]. Verfügbar: https://gdprinformer.com/gdpr-articles/data-protection-training-10-tips-staff.

2.7 LU7 – Sicherheitsprüfung

Lerneinheit 7	Sicherheitsprüfung
Allgemeine Beschreibung / Ausgang	**Installieren Sie eine Firewall und Anti-Virus-Software. Führen Sie Updates durch und wenden Sie grundlegende Methoden an, um die Sicherheit der im Unternehmen eingesetzten Software zu testen und eine entsprechende Dokumentation zu erstellen.**
Code-Nummer	LE 7
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen zu verstehen, wie wichtig es ist, die bestehende IKT-Infrastruktur auf ihre Verwundbarkeit angesichts der technologischen Entwicklungen zu testen. Sie lernen, Penetrationstest-Tools einzusetzen (oder mit externer Unterstützung zu verstehen), um die Sicherheit von Firewalls und Kommunikationskanälen zu gewährleisten. Es gibt eine unendliche Anzahl von Möglichkeiten, eine Anwendung zu knacken. Und Sicherheitstests allein sind nicht das einzige (oder das beste) Maß dafür, wie sicher eine Anwendung ist. Es wird jedoch dringend empfohlen, Sicherheitstests als Teil des Standard-Softwareentwicklungsprozesses durchzuführen.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - über Netzwerksicherheit: Dies beinhaltet die Suche nach Schwachstellen in der Netzwerkinfrastruktur (Ressourcen und Richtlinien). - über die Sicherheit der Systemsoftware: Dies beinhaltet die Bewertung von Schwachstellen in der verschiedenen Software (Betriebssystem, Datenbanksystem und andere Software), von der die Anwendung abhängt. - über Client-seitige Anwendungssicherheit: Hier geht es darum, dass der Client (Browser oder ein solches Tool) nicht manipuliert werden kann. - über die Sicherheit von Server-seitigen Anwendungen: Hier geht es darum, sicherzustellen, dass der Servercode und seine Technologien robust genug sind, um jedes Eindringen abzuwehren. **Können** - Tests erstellen, um die Sicherheit des Softwareprodukts zu bestimmen. - den bestehenden Rahmen anpassen. - Zugriff auf Computersystem oder Netzwerk mit Berechtigung. - sicherstellen, dass die Systeme keine Daten stehlen oder zerstören.

	- die meisten Abbrucharbeiten mit Genehmigung des Eigentümers durchführen. **Persönliche Kompetenz** **Die TeilnehmerInnen sind in der Lage** - die Dokumentation von Prozessen als Ausgangspunkt für weitere Arbeitsschritte zu erkennen. - strukturiert und detailorientiert arbeiten. - die zur Aufgabe gehörende Verantwortung erkennen und sicher im Umgang mit anderen sein.
Empfehlungen für Lernen & Lehren	Die meisten Arten von Sicherheitstests beinhalten komplexe Schritte und Out-of-the-Box-Denken, aber manchmal geht es auch um einfache Tests, die helfen, die schwerwiegendsten Sicherheitsrisiken aufzudecken.
Literatur & weitere Ressourcen	Dekkers, C., McCurley, J., & Zubrow, D. (2013). Measures and Measurement for Secure Software Development. Pittsburgh: Carnegie Mellon University. Dowd, M., McDonald, J., & Schuh, J. (2007). The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Boston: Addison-Wesley.

2.8 LU8 – Kodierung

Lerneinheit 8	Kodierung
Allgemeine Beschreibung / Ausgang	**Arbeiten Sie an der Absicherung von mobilen Geräten, Kommunikationskanälen und Datenspeichern über Passwörter oder andere Mittel der Authentifizierung.**
Code-Nummer	LE 8
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen die Bedeutung der Passwortverschlüsselung für ihre Verwundbarkeit angesichts der technologischen Entwicklungen zu verstehen. Sie lernen, Passwortverschlüsselungs-Tools zu verwenden (oder mit externer Unterstützung zu verstehen), um die Sicherheit von Firewalls und Kommunikationskanälen zu gewährleisten. Die Kennwortverschlüsselung ist der Prozess, bei dem ein Kennwort von einem wörtlichen Textformat in eine für den Menschen unlesbare Zeichenfolge umgewandelt wird. Wenn es richtig gemacht wird, ist es sehr schwierig, zum ursprünglichen Kennwort zurückzukehren, und so hilft es, Benutzeranmeldeinformationen zu sichern und unautorisierten Zugriff auf eine Website zu verhindern.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - über Literal Values: Passwörter wurden im literalen Textformat in Datenbanken gespeichert, ohne jegliche Verschlüsselung oder Hashing. Da Datenbanken eine Authentifizierung benötigen, die niemand außer den Admins und der Anwendung hatte, wurde dies als sicher angesehen. - über Verschlüsselung: Sie ist eine sicherere Alternative und der erste Schritt in Richtung Passwortsicherheit. - über Hashing: Um diese Angriffe zu bekämpfen, mussten sich die Entwickler eine Möglichkeit einfallen lassen, Passwörter in einer Datenbank so zu schützen, dass sie nicht entschlüsselt werden können. - über Salting: Um das Auftreten von Regenbogentabellen zu bekämpfen, begannen die Entwickler, eine zufällige Zeichenfolge an die Anfänge der gehashten Kennwörter anzuhängen. - über Kennwort-Kodierer: Es stehen mehrere Kennwortkodierungsimplementierungen zur Auswahl. Jede hat ihre Vor- und Nachteile, und ein Entwickler kann je nach den Authentifizierungsanforderungen seiner Anwendung wählen, welche er verwenden möchte.

	Können - das Team über die besten Praktiken bei der Passwortverschlüsselung aufklären. - das Team über Cybersicherheit aufklären. - entscheiden, welche Kennworttypen nicht verwendet werden sollen. - die richtige Art und Weise der Erzeugung von Kodierprozessen zu definieren. - komplexe Passwörter beseitigen. - das Risiko des Kopierens eines Passworts stark reduzieren. - Passwortprüfung und -verantwortung sicherstellen. **Persönliche Kompetenz** **Die TeilnehmerInnen sind in der Lage** - erkennen die Dokumentation von Prozessen als Ausgangspunkt für weitere Arbeitsschritte. - strukturiert und detailorientiert arbeiten. - die zur Aufgabe gehörende Verantwortung erkennen und sicher im Umgang mit anderen sein. - die wichtigsten geforderten Aufgaben mit einem guten Maß an Selbstständigkeit zu bewältigen. - ihre sozialen Kompetenzen (insbesondere Soft Skills, Empathie und Kommunikation) betonen.
Empfehlungen für Lernen & Lehren	Die meisten Arten von Kodierungsprozessen erfordern komplexe Schritte und unkonventionelles Denken, aber manchmal sind es einfache Tests wie der oben beschriebene, die helfen, die schwerwiegendsten Kodierungsrisiken aufzudecken.
Literatur & weitere Ressourcen	Kaliski, B. (2000). Password-Based Cryptography Specification Version 2.0. RFC Editor, US. https://doi.org/10.17487/RFC2898. Mourouzis, T., Pavlou, K. E., & Kampakis, S. (2018). The Evolution of User-Selected Passwords: A Quantitative Analysis of Publicly Available Datasets. Computer Science. arXiv:1804.03946. Barbero, G., Trasselli, F. (2015). Manus OnLine und das Text Encoding Initiative Schema. Journal of the Text Encoding Initiative, (8), 1-16. doi: 10.4000/jtei.1054.

2.9 LU9 – Daten Management

Lerneinheit 9	Daten Management
Allgemeine Beschreibung / Ausgang	**Führen Sie routinemäßige Backups von Daten durch und wenden Sie Methoden des ordnungsgemäßen Verhaltens gemäß DSGVO auf die Datenverarbeitung im Unternehmen an.**
Code-Nummer	LE 9
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen zu verstehen, wie wichtig es ist, Daten und Informationen gemäß den vereinbarten Richtlinien zu speichern und zu verarbeiten. Sie lernen den richtigen Umgang mit Daten unter Berücksichtigung der DSGVO kennen. Die TeilnehmerInnen werden in die Lage versetzt, die Speicherung und Verarbeitung von physischen und elektronischen Daten im Unternehmen zu bewerten und potenzielles Fehlverhalten zu erkennen. Die TeilnehmerInnen lernen, Änderungen in den Firmenprozessen vorzuschlagen, um diese Risiken zu mindern.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - wie man den Informationsbedarf für den erfolgreichen Prozess definiert: welche Art von Daten werden im Unternehmen verarbeitet und welche Speichertechniken sollten den jeweiligen Vorschriften entsprechen. - Regeln, wie Umfang und Zweck der Speicherung und Verarbeitung personenbezogener Daten zu bestimmen sind. - wie man Datenmanagement im Unternehmen organisiert und anwendet: sich dem Wandel anpassen; analytisches Denken anwenden; Lösungen entwickeln; Projektmanagementaufgaben selbständig durchführen. - verschiedene Techniken und Kommunikationsstile, um notwendige Informationen über die Speicherung zu erhalten. **Können** - den Umfang und den Zweck der personenbezogenen Daten zu bestimmen, die innerhalb der Organisation gespeichert/verarbeitet werden. - erstellen Sie regelmäßig Backups, um das Risiko des Verlusts wertvoller Daten und Informationen zu minimieren. - Arbeit innerhalb der Gruppe zur effizienten Gewinnung von Informationen zur Verbesserung von Prozessen. - verschiedene Ressourcen zu planen und zu verwalten und den Datenverwaltungsprozess zu überwachen, um ein bestimmtes Ziel zu erreichen.

	Persönliche Kompetenz **Die TeilnehmerInnen sind in der Lage** - strukturiert und detailorientiert arbeiten. - die zur Aufgabe gehörende Verantwortung erkennen und sicher im Umgang mit anderen sein. - Aufgaben selbständig erledigen und Lernbereitschaft zeigen.
Empfehlungen für Lernen & Lehren	Kombinieren Sie theoretisches Wissen und Vorgehen mit praktischen Beispielen. Interaktive Lehrmethoden anwenden (z. B. Gruppenarbeit, Diskussionen, Fallanalysen, Simulationsrollenspiele usw.)
Literatur & weitere Ressourcen	Calabro, A., Daoudagh, S., & Marchetti, E. (2020). Gestaltungsprinzipien für die General Data Protection Regulation (GDPR): Eine formale Konzeptanalyse und ihre Bewertung. Information Systems (91) [Online]. Verfügbar: https://www.sciencedirect.com/science/article/pii/S0306437919305216. Guide on Good Data Protection Practice in Research (2019) [Online]. Verfügbar: https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf. EU-GDPR. (2019). EU-GDPR-Portal. [Online]. Verfügbar: https://eugdpr.org. Allgemeine Datenschutzverordnung (2018). Amtsblatt der Europäischen Union [Online]. Verfügbar: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

2.10 LU10 – Rollenbasierte Zugriffskontrolle

Lerneinheit 10	Rollenbasierte Zugriffskontrolle
Allgemeine Beschreibung / Ausgang	**Richten Sie Administratorkonten ein und schränken Sie die Zugriffsrechte der Mitarbeiter entsprechend den definierten Sicherheitsstufen ein.**
Code-Nummer	LE 10
Typ	Obligatorisch - muss definiert werden
Ausmaßxs	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen zu verstehen, wie wichtig es ist, den Zugriff auf Daten, Informationen oder die physische Infrastruktur, wenn möglich einzuschränken und nur einer Gruppe von relevanten Mitarbeitern Zugang zu gewähren. Sie lernen, wie man angemessene Einschränkungen entsprechend einer definierten Sicherheitsstufe festlegt. Die TeilnehmerInnen werden in die Lage versetzt, Rollen innerhalb des Unternehmens den Freigabestufen zuzuordnen und den Zugriff auf bestimmte Informationen bei Bedarf nachvollziehbar zu machen.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - wie man die wichtigsten Vorgänge mit personenbezogenen Daten identifiziert, die innerhalb einer Organisation durchgeführt werden. - wie man die Zugänglichkeit von Informationen für bestimmte Mitarbeitergruppen herstellt. - wie man angemessene Einschränkungen gemäß den definierten und vereinbarten Sicherheitsstufen einrichtet, wenn dies als notwendig erachtet wird. **Können** - die Rollen einzelner Mitarbeiter und Gruppen zu unterscheiden, um ihre Bedürfnisse für verschiedene Sicherheitsstufen zu definieren (basierend auf zugewiesenen Sicherheitsstufen, die mit der Geschäftsleitung vereinbart wurden). - für einzelne Mitarbeiter oder Gruppen geeignete Lösungen in Bezug auf Zugang oder Einschränkungen finden und diese begründen können. - die Verwaltung individueller Benutzerrechte, die einfach durch die Zuweisung geeigneter Rollen zum Benutzerkonto erfolgt, wenn die Rollen klar definiert sind (durch das Management).

	Persönliche Kompetenz **Die TeilnehmerInnen sind in der Lage** - selbstständig entsprechende Rollen nach den Vorgaben des Managements zuweisen (zugewiesene Sicherheitsstufen). - selbstbewusst mit KollegInnen und der Geschäftsleitung zu kommunizieren, indem sie sicher im Umgang miteinander sind. - selbständig die zur Aufgabe gehörende Verantwortung erkennen und die Bedürfnisse anderer respektieren.
Empfehlungen für Lernen & Lehren	Lernen Sie die drei primären Regeln, die für RBAC definiert sind, kennen bzw. lehren Sie sie: 1) Rollenzuweisung, 2) Rollenautorisierung, 3) Berechtigungsautorisierung. Denken Sie an die Bedeutung der Sensibilisierung bei der Rollenzuweisung und treffen Sie klare Vereinbarungen mit dem Management.
Literatur & weitere Ressourcen	Blokdyk, G., (2017). Rollenbasierte Zugriffskontrolle: Ein erfolgreicher Design-Prozess. D Ferraiolo, DR Kuhn, R Chandramouli, (2003), Role-based access control. Benantar, M., (2006), Access Control Systems: Sicherheit, Identitätsmanagement und Vertrauensmodelle. New York: Springer. Zhang, E. (2020). Was ist Role-Based Access Control (RBAC)? Beispiele, Vorteile und mehr [Online]. Verfügbar: https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more.

2.11 LU11 – Passwort Management

Lerneinheit 11	Passwort Management
Allgemeine Beschreibung / Ausgang	**Legen Sie Passwörter für den individuellen Zugriff der Mitarbeiter fest und sorgen Sie für eine sichere Speicherung und Wiederherstellung.**
Code-Nummer	LE 11
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen zu verstehen, wie wichtig es ist, die Verwaltung der Passwortnutzung im Unternehmen zu zentralisieren. Sie lernen, wie man Passwörter definiert, die die Authentifizierung (unter den Mitarbeitern) sicherstellen und wie man Passwörter zurücksetzt. Die TeilnehmerInnen lernen, wie sie Passwörter von Mitarbeitern strukturell erstellen, verwenden/verwalten, speichern und ändern können.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - über die Speicherung von Passwörtern. - über die Übertragung des Passworts. - über das Erraten von Passwörtern. - über das Knacken von Passwörtern. - über das Ersetzen von Passwörtern. **Können** - das Team über die besten Praktiken bei Passwörtern schulen. - das Team über Cybersicherheit aufklären. - entscheiden, welche Kennworttypen nicht verwendet werden sollen. - komplexe Passwörter generieren. - Nutzen Sie die Kraft der Automatisierung. - komplexe Passwörter beseitigen. - eliminieren die Notwendigkeit, Passwörter neu zu setzen. - Passwortprüfung und -verantwortung sicherstellen. **Persönliche Kompetenz** **Die TeilnehmerInnen sind in der Lage** - die Dokumentation von Prozessen als Ausgangspunkt für weitere Arbeitsschritte zu erkennen. - strukturiert und detailorientiert arbeiten. - die zur Aufgabe gehörende Verantwortung erkennen und sicher im Umgang mit anderen sein.

	- die wichtigsten geforderten Aufgaben mit einem guten Maß an Selbstständigkeit zu bewältigen. - ihre sozialen Kompetenzen (insbesondere Soft Skills, Empathie und Kommunikation) zu betonen.
Empfehlungen für Lernen & Lehren	Passwortverwaltung mit Hilfe von Beispielen aus der Praxis. Übungen zur Dokumentation in freier Form und mit Hilfe von Textbausteinen.
Literatur & weitere Ressourcen	Luca, M. (2008). Passwortmanagement für verteilte Umgebungen. Saarbrücken: VDM Verlag Dr. Müller. Smith, S. B. (2017). Passwort-Manager: Internet-Benutzer-ID und Passwörter im Passwort-Manager aufbewahren. Bewahren Sie Ihre Internet-Anmeldeinformationen an einem sicheren Offline-Ort auf. CreateSpace: North Charleston.

2.12 LU12 – Business Continuity Management

Lerneinheit 12	Business Continuity Management
Allgemeine Beschreibung / Ausgang	**Legen Sie Richtlinien und Verfahren für das Auftreten von möglichen Eventualitäten fest.**
Code-Nummer	LE 12
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen, die Bedeutung der Durchführung von "Was wäre wenn"-Szenarien zu verstehen. Sie lernen, theoretische Eventualitäten zu analysieren und entsprechend strategische Leitlinien zu erstellen. Die TeilnehmerInnen werden in die Lage versetzt, Richtlinien zu erstellen und Maßnahmen vorzudefinieren, um auf neue Situationen vorbereitet zu sein und koordiniert zu reagieren, wenn diese eintreten.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - wie man nationale Dokumente findet und wie man in nationalen Rechtsdokumenten, die Sicherheit und Datenschutz regeln, nach Wissen sucht. - Simulationstechniken, um potenzielle Datenverletzungen vorhersehen zu können. - wie man mit Regeln zur Risikobeurteilung umgeht. **Können** - Risiken mit verschiedenen Techniken und Kommunikationsstilen zu identifizieren. - Regeln zur Risikobeurteilung einführen, die mit Zustimmung der Geschäftsleitung handeln. - planen und entwickeln Lösungen, die sich an die Gegebenheiten und Veränderungen in der Organisation anpassen, und setzen diese mit Zustimmung der Geschäftsleitung um. - neue Lösungen auf der Grundlage der Analyse früherer Ereignisse zu finden. **Persönliche Kompetenz** **Die TeilnehmerInnen sind in der Lage** - unter ungünstigen Umständen arbeiten und dabei an den Details hängen bleiben. - sich leicht an neue Gegebenheiten anpassen. - ein Beispiel für andere Mitarbeiter zu sein, die ihrem ethischen Verhaltenskodex folgen und Verantwortung zeigen.

	-
Empfehlungen für Lernen & Lehren	Theoretisches Üben von Szenarien verschiedener Bedrohungen und Risikosituationen. Arbeiten mit Beispielen aus realen Situationen.
Literatur & weitere Ressourcen	Irwin, L. (2019). Warum Risikobewertungen für die Einhaltung der GDPR unerlässlich sind [Online]. Verfügbar: https://www.itgovernance.co.uk/blog/why-risk-assessments-are-essential-for-gdpr-compliance. European Data Protection Board (2021). Guidelines 01/2021 on Examples regarding Data Breach Notification [Online]. Verfügbar: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf. European Union Agency for Cybersecurity (2017). Handbook on Security of Personal Data Processing [Online]. Verfügbar: www.enisa.europa.eu. Green, A. (2020). GDPR Data Breach Guidelines - COMPLIANCE & REGULATION [Online]. Verfügbar: https://www.varonis.com/blog/guide-eu-gdpr-breach-notification-rule/. Allgemeine Datenschutzverordnung (2021). Vollständiger Leitfaden zur Einhaltung der GDPR [Online]. Verfügbar: https://gdpr.eu/.

2.13 LU13 – Mediation und Stakeholder-Management

Lerneinheit 13	Mediation und Stakeholder-Management
Allgemeine Beschreibung / Ausgang	**Koordinieren Sie die Bedürfnisse von Führungskräften und Mitarbeitern des Unternehmens und versorgen Sie beide Parteien mit Informationen und Einblicken aus dem Unternehmen.**
Code-Nummer	LE 13
Typ	Obligatorisch - muss definiert werden
Ausmaß	Stunden - noch zu definieren
Handlungs-kompetenzen	Die TeilnehmerInnen lernen zu verstehen, wie wichtig es ist, sich mit allen Beteiligten im Unternehmen hinsichtlich ihrer Rolle und ihres Einflusses auf Datenschutz und Informationssicherheit abzustimmen. Sie lernen, wie man effektiv mit verschiedenen Hierarchieebenen (Mitarbeiter und Management) kommuniziert und deren Bedürfnisse und Interessen bei Änderungen von Organisationsabläufen abgleicht. Die TeilnehmerInnen werden in die Lage versetzt, mit Stakeholdern diplomatisch zu interagieren und mit möglichen Widerständen gegen die eigene Einflussnahme umzugehen.
Lernergebnisse	**Technische Kompetenz** Die TeilnehmerInnen **Wissen** - wie man nationale Rechtsdokumente findet, die Informationssicherheit und Datenschutz regeln und wie man nach Wissen sucht. - welche internen und externen Kommunikationskanäle mit Zustimmung des Managements eingesetzt werden dürfen und welche Risiken damit verbunden sind. - welche Maßnahmen zur Beobachtung, Prüfung und Bewertung von Prozessen in der Organisation eingesetzt werden können. - welche Maßnahmen zur Risikobeurteilung angewendet werden können und wie man mit der Risikobeurteilung umgeht. **Können** - Maßnahmen der internen Revision umsetzen (mit Zustimmung der Geschäftsführung). - planen und entwickeln strategische Lösungen und setzen diese dann handelnd mit Zustimmung des Managements um. - Installieren Sie eine Präventionskultur mit Unterstützung des Managements. - Risiken zu identifizieren, zu bewerten und zu priorisieren. - interne Regelungen auf organisatorischer Ebene zu erstellen und diese (mit Zustimmung der Geschäftsleitung) umzusetzen.

	Persönliche Kompetenz **Die TeilnehmerInnen sind in der Lage** - Umgang mit Veränderung und Anpassung. - kreativ sein und sich weiterentwickeln wollen. - sich auf ihren eigenen ethischen Kodex verlassen, damit andere ihrem Beispiel folgen können. -
Empfehlungen für Lernen & Lehren	Kombinieren Sie theoretisches Wissen und Vorgehen mit praktischen Beispielen. Interaktive Lehrmethoden anwenden (z. B.: Gruppenarbeit, Diskussionen, Fallanalysen, Simulationsrollenspiele, etc.)
Literatur & weitere Ressourcen	IT Governance Privacy Team (2020). EU General Data Protection Regulation (GDPR) - An implementation and compliance guide (4th ed.). Allgemeine Datenschutzverordnung (2021). Vollständiger Leitfaden zur Einhaltung der GDPR [Online]. Verfügbar: https://gdpr.eu/. Gorondutse, A. H., & Hilman, H. (2016). Mediationseffekt der Organisationskultur auf die Beziehung zwischen wahrgenommener Ethik und KMU. Journal of Industrial Engineering and Management 2016, 9(2), 505-529. Straight, J. (2018). GDPR compliance: Identifizierung des einzigartigen Profils einer Organisation [Online]. Verfügbar: https://www.helpnetsecurity.com/2018/05/14/gdpr-compliance-profile/

Curriculum

We thank the co-authors and from:

BF/M-Bayreuth

Mykolas Romeris University

WSBiNoZ

Consulenza Direzionale di Paolo Zaramella

Hafelekar Unternehmensberatung

Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeISi

Funded by the Erasmus+ Programme of the European Union

https://information-security-in-sme.eu/.