Curriculum – Lietuvių

Žinių, įgūdžių ir gebėjimų, susijusių su informacijos saugumu ir duomenų apsauga MVĮ, mokymosi vienetai

Funded by the
Erasmus+ Programme
of the European Union

TeBelSi

Funded by the
Erasmus+ Programme
of the European Union

Šis dokumentas parengtas įgyvendinant ERASMUS+ projektą "Teilzertifizierung im Berufsfeld Informationssicherheit - TeBeiSi", projekto ID: 2018-1-EN02-KA202-005218

Turinys

Funded by the
Erasmus+ Programme
of the European Union

1 TeBeISI – Trumpai apie projektą

IT sektoriui paprastai būdingi trumpi kūrėjų ir gamintojų inovacijų ir produktų ciklai. Dėl nuolat besikeičiančių IT sektoriaus reikalavimų mokymasis ir neformalių aspektų pripažinimas tampa lemiamu veiksniu ir informacijos saugumo srityje. Sertifikavimo galimybių trūkumas lemia informacijos saugumo srities specialistų trūkumą (visame pasaulyje). Ši problema žinoma jau daugelį metų ir kelia rimtų iššūkių ekonomikai. Todėl „Betriebswirtschaftliches For-schungszentrum für Fragen der mittelständischen Wirtschaft e. V.“ (BF/M-Bayreuth) pradėjo vykdyti bendrą Europos projektą TeBeISi - "Dalinis sertifikavimas informacijos saugumo profesinėje srityje", kurio tikslas - nustatyti ir įvertinti kompetencijas informacijos saugumo srityje. Visoje Europoje vienodas neformaliai įgytų kvalifikacijų vertinimas ir pripažinimas turi didžiulį potencialą kovojant su kvalifikuotų darbuotojų trūkumu informacijos saugumo srityje.

Projektas padeda skatinti kvalifikacijų ir kompetencijų, įskaitant įgytas neformaliojo mokymosi ir savišvietos būdu, pripažinimą ir sertifikavimą. Vykdant Europos institucijų mainus, keičiantis patirtimi, bus apdorojami ir į naujai sukurtus profesijų profilius įtraukiami profesijų profilių, kurie konkrečiai vyrauja šalyse, sertifikavimai. Projektu siekiama šiuos profilius, įskaitant sertifikavimo procedūras, perkelti į Europos šalis partneres ir sėkmingai įgyvendinti praktikoje. Daugiausia dėmesio skiriama neformaliojo ir savaiminio mokymosi rezultatų patvirtinimui.

Projektui įgyvendinti reikėjo daug priemonių. Siekiant nustatyti reikalingas informacijos saugumo kompetencijas, buvo atlikta išsami literatūros analizė, ekspertų interviu ir fokus grupės su įmonėmis. Šių išvadų pagrindu buvo sudarytas reikalavimų katalogas. Siekiant bendrų sutarimų tinkamų visoje Europoje, reikėjo parengti rekomendacijas dėl veiksmų. Tai buvo daroma, be kita ko, įtraukiant asociacijas ir asocijuotus partnerius iš ekonomikos. Kitas žingsnis buvo internetinio personalo klausimyno, skirto informacijos saugumo kompetencijoms nustatyti, sukūrimas, daugiausia dėmesio skiriant socialinėms kompetencijoms.

Kitas svarbus projekto etapas, kuris detaliai pristatomas šiame leidinyje, yra mokymo modulių, skirtų konkrečioms dalinėms kompetencijoms ugdyti(s), kūrimas, atsižvelgiant į socialinius ir techninius komponentus: TeBeISi mokymo programa.

Pagrindinis projekto baigiamojo etapo produktas – strateginis dokumentas, parengtas remiantis naujuoju duomenų apsaugos reglamentu, sąvokų žodynėlis taikymui ir tyrimo ataskaita "Status Quo informacijos saugumo mokymai mažoms ir vidutinėms įmonėms (MVĮ)".

1.1 Projekto partneriai:

- BFM - Betriebswirtschaftliches Forschungszentrum Mittelstand (Germany): www.bfm-bayreuth.de
- Hafelekar Unternehmensberatung – (Austria): http://www.hafelekar.at
- Consulenza Direzionale Paolo Zaramella (Italy): https://www.linkedin.com/in/paolozaramella
- MRU - MYKOLAROMERIS UNIVERSITY (Lithuania): www.mruni.eu
- WSBINOZ (Poland): www.medyk.edu.pl

2 TeBelSi mokymo programos kūrimo parengiamieji etapai

2.1 1 etapas (IO1) - kompetencijų profilių nustatymas

Visos penkios dalyvaujančios organizacijos užsibrėžė tikslą išsiaiškinti, kokius konkrečius reikalavimus MVĮ kelia informacijos saugumo ir duomenų apsaugos srityse. Informacijos saugumo ir duomenų apsaugos kompetencijų poreikio nustatymas kiekvienoje šalyje partnerėje prasidėjo nuo tyrimo atlikimo: organizacijos partnerės pakvietė ekspertus pokalbiams ir surengė tikslinių grupių susitikimus, kad sužinotų daugiau apie realius (vietos) MVĮ poreikius. Šios veiklos rezultatais remtasi rengiant "Kompetencijų profilių nustatymo ataskaitą", kuria siekta toliau nustatyti reikalingas kompetencijas tiek informacijos saugumo, tiek duomenų apsaugos srityje.

Diagramoje pateikiami ekspertų nuomonių rezultatai: grafike pavaizduoti žodžiai ir frazės - tai dažniausiai pateikti atsakymai į klausimą apie jų darbui reikalingus įgūdžius ir kompetencijas. Kuo didesnis šriftas, tuo dažniau buvo įvardytas atsakymas:

Figure 1: Simon Rath, BFM: Kodavimo debesis - sukurtas iš dokumentų ir tyrimų duomenų

2.2 2 etapas (IO3) - internetinis klausimynas

Preliminarūs rezultatai, gauti atlikus tyrimus, buvo patikslinti ir tapo pagrindu pirmajam mokymosi modulių projektui. Siekiant peržiūrėti ir išplėsti partnerystės poreikių analizę (kaip IO1 rezultatą), buvo parengtas internetinis klausimynas, kad būtų galima: 1) patikrinti projekto rezultatus; 2) geriau suprasti, kokių kompetencijų reikia MVĮ; 3) nustatyti kompetencijų lygių nuorodas kiekvieno padalinio subkompetencijoms (kurias galima naudoti savęs vertinimui); 4) apžvelgti, kokias strategijas (jei apskritai tokias taiko) MVĮ taiko, kad įveiktų darbo jėgos trūkumą.

Todėl internetinį klausimyną sudaro dvi dalys: pats klausimynas, skirtas įmonių vadovams, darbuotojams, dirbantiems žmogiškųjų išteklių ir IT srityse, taip pat bendriesiems MVĮ darbuotojams. Atsižvelgiant į jų funkcijas įmonėje, klausimynas pritaikomas taip, kad kiekvienai grupei būtų pateiktas tinkamas klausimų rinkinys, užtikrinant, kad, pavyzdžiui, į klausimus, atitinkančius MVĮ informacijos saugumo mokymo programą, atsakinėtų tik ekspertai. Antroji dalis - tai savęs vertinimo priemonė. Įrankis leidžia įmonėms pasitikrinti, kokių kompetencijų joms reikia (priklausomai nuo jų naudojamų technologijų, taip pat tam tikrų atliekamų užduočių kiekio ir svarbos), ir konkrečiai savarankiškai įvertinti atitinkamus padalinius. Taip galima užtikrinti, kad vertinamos tik svarbios kompetencijos, o tai patvirtina projekto grupės nuostatą, kad savęs vertinimas būtų kuo trumpesnis ir paprastesnis.

Tikslų klausimyno turinį sudaro elementai, kuriais siekiama įvertinti rinkos paklausą, kartu su elementais, kylančiais iš parengto klausimyno. Pastarajame išskaidomos kiekvieno iš 13 modulių subkompetencijos ir prašoma dalyvių atlikti savęs vertinimą (tiek įmonės poreikio, tiek savo gebėjimų). Visas surinktų duomenų rinkinys bus naudojamas ataskaitai "Status Quo - informacijos saugumas MVĮ" parengti.

Darbo su šiomis priemonėmis procedūra yra tokia: pirmiausia, siekiant surinkti reikiamus duomenis, didysis klausimynas buvo išplatintas šalių partnerių įmonėms ir valdžios institucijoms. Antra, duomenys buvo įtraukti į savęs vertinimo priemonę, kuri bus pateikta visoms suinteresuotoms įmonėms. Lengvai naudojamą priemonę svarbu pateikti atsižvelgiant į tai, kad įveikdamos įgūdžių trūkumą įmonės turi investuoti laiko ir išteklių. Kuo paprasčiau bus naudojamasi priemone, tuo didesnio pritarimo tikimasi.

3 „TeBelSi“ mokymų programa

Mokymo tikslas - suteikti MVĮ išteklių, kurie atitiktų konkrečią darbo jėgos paklausą. Iš dalinio sertifikavimo idėjos kylanti mokymo programa, pagal kurią galima mokyti labai konkrečių gebėjimų, suteikia besimokantiesiems galimybę atlikti tam tikras konkrečias užduotis. Įvertinus ekonominius dalinio sertifikavimo privalumus, asmeniui nereikia išklausyti viso kurso (pvz., mokytis 3 metus), nors didžiąją dalį kvalifikacijai reikalingų kompetencijų jis jau turi. Tikrovėje yra priešingai, ir asmenys susilaiko nuo kursų naštos, kad patvirtintų savo kompetencijas. Ceteris paribus, įmonės yra labiau linkusios investuoti į konkrečiai joms reikalingų kompetencijų mokymą, nes kvalifikacijos kėlimo procesas jų požiūriu yra efektyvesnis laiko atžvilgiu ir ekonomiškesnis.

3.1 Kam skirta ši kvalifikacijos tobulinimo programa?

Mokymų tikslinė grupė yra dvejopa: 1) įmonės, siekiančios užpildyti labai konkrečią paklausą 2) asmenys, norintys įgyti kompetencijų informacijos saugumo ir duomenų apsaugos srityje, daug dėmesio skiriant į veiksmus orientuotiems gebėjimams. Pirmąją grupę sudaro visų ES ekonominių sektorių MVĮ, o antrąją - įvairūs besimokantieji, nesvarbu, ar tai būtų universitetų studentai, norintys įgyti papildomą kvalifikaciją, ar besimokantieji pagal profesinio mokymo programas, kuriems reikia įgyti naujų gebėjimų, kuriuos būtų galima įtraukti į esamą mokymo programą, ar darbuotojai, siekiantys išplėsti savo įsidarbinimo galimybes.

Visoms šioms grupėms keliami panašūs dalyvavimo mokymų programoje reikalavimai:

- Ar mokymų dalyviai jau turi būti formaliuoju mokymosi būdu įgiję kvalifikaciją?
    - Ne. Mokymų programa atvira visiems, tiek dar studijuojanties, tiek jau dirbantiems. Būtina tik tam tikra patirtis (pvz., praktinio veikimo tam tikroje srityje patirtis, IKT išmanymas ir pan.).
- Ar dalyviams būtina turėti žinių informacijos saugumo ir duomenų apsaugos srityje?
    - Ne. Mokymų dalyviai turi gebėti skaityti ir suprasti dokumentus, susijusius su indormacijos saugumu ir duomenų apsauga. IKT išmanymas yra naudingas.

3.2 Kokios šios kvalifikacijos tobulinimo programos įgyvendinimo formos?

Konkretus kurso dizainas priklauso nuo švietimo įstaigų tikslinės grupės. Mokymų programa turi numatyti kurso turinį, o kaip jis bus perteikiamas ar realizuojamas gali spręsti pati mokymus organizuojanti įstaiga. Siūlytinos dvi mokymų organizavimo formos: nuotolinis mokymas(is) ir mišrus mokymas(is). Mokomosios medžiagos parengimas nėra „TeBelSi“ projekto veiklos sritis. Mokymų paslaugų teikėjai gali laisvai nuspręsti, kiek laiko jie nori skirti atskiriems mokymosi moduliams, jų turinio realizavimui.

4 „IS-DA praktikuojančio MVĮ“ darbo aprašymas

Informacijos saugumo ir duomenų apsaugos specialistas MVĮ, toliau vadinamas „IS-DA praktikuojančiu asmeniu, atlieka vadovybę ir (arba) IT skyrių papildantį vaidmenį ir, glaudžiai bendradarbiaudamas su vadovybe, siekia apsaugoti įmonę nuo bet kokios žalos, kurią tiesiogiai sukeltų duomenų apsaugos pažeidimai arba informacijos praradimas dėl saugumo sistemos pažeidimų. Atitinkama kompetencija suteikia MVĮ galimybę naudotis darbuotojais, kurie yra pakankamai kvalifikuoti atsižvelgiant į jų konkrečius poreikius, priklausomai nuo to, kaip jos dirba, kokias technologijas naudoja ir kokius duomenis tvarko. Konkrečiai MVĮ turi būti sudarytos palankesnės sąlygos perkvalifikuoti įmonės darbuotoją, kad jis galėtų užimti informacijos saugumo ir duomenų apsaugos srities pareigas ir stiprinti savo techninius gebėjimus.

Informacijos saugumas ir duomenų apsauga, palyginti su didelėmis įmonėmis, MVĮ kelia visai kitokius reikalavimus: komunikacijos kanalai nėra tokie sudėtingi, duomenų rūšis ir kiekis gali būti tvarkomi pagal BDAR atitinkančius standartizuotus procesus, o verslo modelis apskritai yra daug mažiau priklausomas nuo technologinių procesų. Todėl darbuotojo, kuriam pavesta atlikti duomenų apsaugos ir informacijos saugumo pareigas, įgūdžiai, reikalingi dirbant MVĮ, labai pasikeičia, nors pagrindiniai darbo tikslai išlieka tokie patys kaip ir didelėse įmonėse.

Atsižvelgiant į tai, siūlomas IS-DA praktiko kompetencijų rinkinys leidžia darbuotojui atlikti užduotis, atitinkančias informacijos saugumo MVĮ reikalavimus. Nepaisant to, reikia įgyti įvairių kompetencijų. Jos apima tiek funkcinius, tiek tarpasmeninius aspektus. Šios kompetencijos ypatingai svarbios tam, kad įmonė būtų informuota apie IS ir DA užtikrinimo procesus ir taip sumažintų galimų grėsmių riziką. Todėl būtina įmonėse rasti darbuotojus, turinčius stiprią socialinę ir savarankišką kompetenciją, kad užimtų šias pareigas.

Siūlomas kompetencijų profilis leidžia MVĮ patenkinti savo specifinius informacijos saugumo poreikius, atsižvelgiant į procesus, technologijas ir darbo aplinką. Darbuotojas, atsakingas už informacijos saugumą ir duomenų apsaugą, neturi nei diegti sertifikavimui paruoštos informacijos saugumo valdymo sistemos, nei nuodugniai analizuoti ir diegti naujų sudėtingų technologinių sprendimų įmonėje. Pagrindinė šio darbuotojo atsakomybė - užtikrinti, kad įmonės darbuotojai būtų susipažinę su informacijos saugumu ir duomenų apsauga, kad būtų taikomi pagrindiniai draudimai, apsaugantys įmonę nuo bet kokios žalos, ir kad saugumo aspektai būtų įtraukti į įmonės strateginę plėtrą. IS-DA specialistas turi padėti vadovybei, nes jis atlieka ryšių tarp vadovų ir darbuotojų palaikymo funkciją.

5 Mokymų programos modulių kūrimas (MM)

Aprašėme procesą, kurio metu buvo apibrėžtas aiškus mokymosi turinys ir mokymosi rezultatai. Taip pat analizavome šiuos klausimus: ko reikia informacijos saugumo specialistams mažosiose ir vidutinėse įmonėse? Kokios kompetencijos yra būtins? Kurios kompetencijos yra aktualesnės didelėse įmonėse? Atlikusi ekspertų interviu, projekto grupė nustatė 13 sričių, kurios apima skirtingas informacijos saugumo specialisto kompetencijos sritis. Remiantis šiomis sritimis galima sukurti mokymosi modulius (MM), kurie leistų besimokantiesiems įgyti visas svarbias kompetencijas, reikalingas pagrindinėms saugumo užtikrinimo priemonėms MVĮ įgyvendinti.

Remiantis ekspertų išskirtomis kompetencijomis tampa visiškai aišku, kad socialinės kompetencijos yra labai svarbios sėkmingai informacijos saugumo specialistų veiklai. Tuo tarpu tiek teisinių aspektų srityje, tiek IKT srityje būtina įvaldyti įvairias technines kompetencijas, o socialinės ir savikompetencijos darbdavių vertinamos kaip būtina sąlyga. Pirmųjų galima išmokti, o specifinis požiūris ir motyvaciniai aspektai, atsirandantys dirbant įmonėje su kitais darbuotojais, yra vertingas turtas, kuris kritinėse situacijose tampa privalomas.

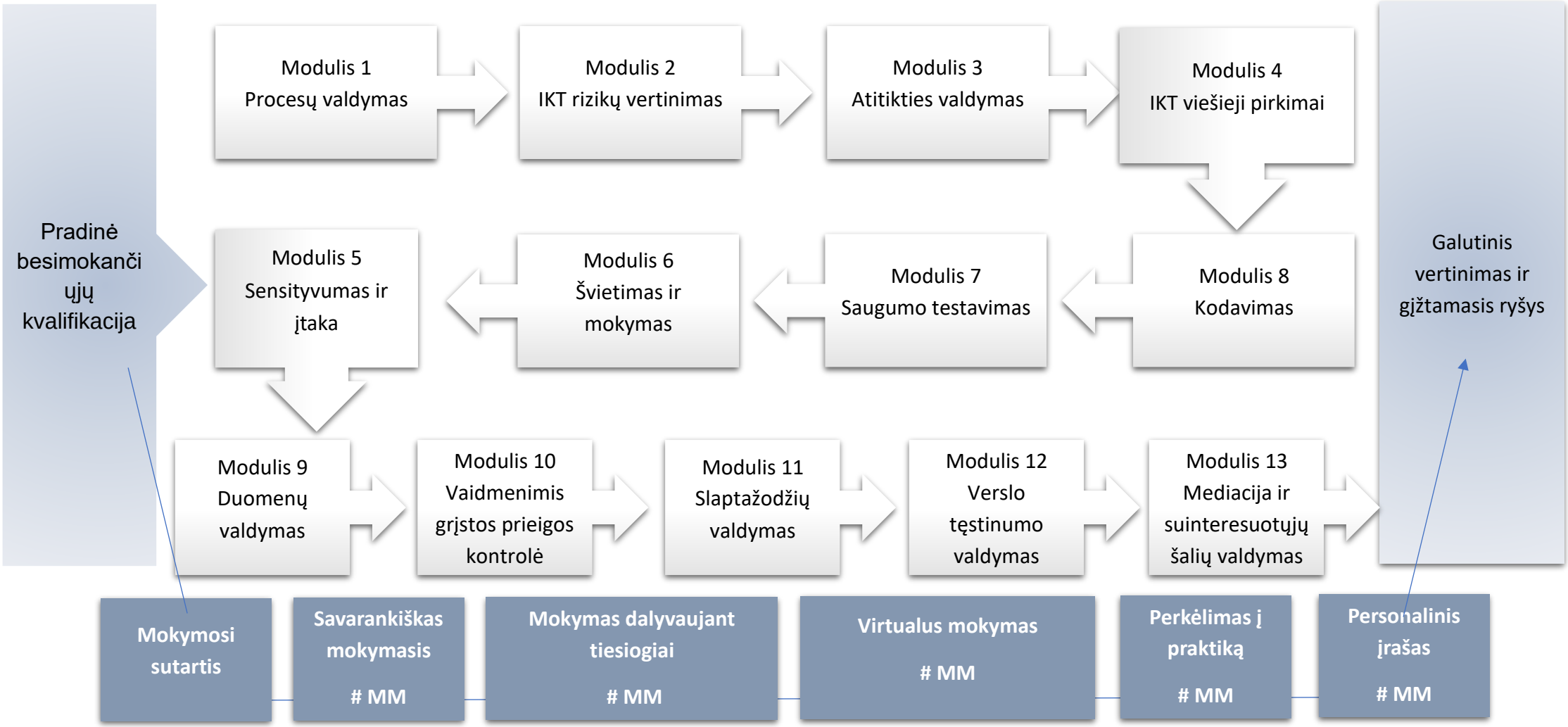
5.1 Mokymosi modulių diagrama (remiantis Europos profesinio mokymo kreditų sistema - ECVET)

Remiantis šia išvada ir laikantis procedūrinio požiūrio, užduotys galėtų būti grupuojamos į mokymosi modulius, apimančius visą informacijos saugumo atsakomybių spektrą, ir grindžiamos pagrindinėmis konkrečiomis kompetencijomis. Šie moduliai gali būti naudojami mokymo tikslais, nesvarbu, ar tai būtų esami įmonės darbuotojai, siekiantys prisiimti naujas pareigas, ar universiteto studentai, siekiantys išplėsti savo įsidarbinimo galimybes, ar kitos besimokančiųjų grupės, norinčios persikvalifikuoti. Taip pat, formalios kvalifikacijos neturintys specialistai, pavyzdžiui, iš profesinio ar aukštojo mokslo įstaigų, gali naudoti šiuos modulius kaip savo kvalifikacijos kriterijus.

Funded by the Erasmus+ Programme of the European Union

TeBelSi

TeBelSi Mokymų planas (remiantis ECVET kriterijais)



5.2 Mokymų moduliai - apžvalga ir trumpas aprašymas

#	Mokymų moduliai	Trumpas aprašymas
MM1	**Procesų valdymas**	Verslo procesų analizė ir strateginės duomenų apsaugos ir informacijos saugumo ataskaitos rengimas.
MM2	**IKT rizikų vertinimas**	Įmonės pokyčių, kurie turi įtakos įmonės saugumo strategijai stebėsena ir ataskaitos kolegoms rengimas.
MM3	**Atitikties valdymas**	Įmonės gairių, kaip elgtis su konkrečia informacija ir duomenimis parengimas.
MM4	**IKT pirkimai**	Rekomendacijų dėl įsigyjamų daiktų parengimas, atsižvelgiant į įmonės informacijos saugumo ir duomenų apsaugos reikalavimus.
MM5	**Sensityvumas ir įtaka**	(Informavimo) veiklų vykdymas, siekiant atkreipti darbuotojų dėmesį į saugumo rizikas ir sužadinant darbuotojų sąmoningumą.
MM6	**Švietimas ir mokymas**	Įmonės mokymo planų parengimas, siekiant vykdyti reguliarius darbuotojų mokymus informacijos saugumo ir duomenų apsaugos srityse.
MM7	**Saugumo testavimas**	Antivirusinės programinę įrangos ir užkardos įdiegimas. Atnaujinimų atlikimas ir pagrindinių metodų pritaikymas, užtikrinant įmonėje naudojamos programinės įrangos saugumą ir atitinkamų dokumentų pateikimą.
MM8	**Kodavimas**	Mobiliųjų prietaisų, ryšio kanalų ir duomenų saugojimo įrenginių sekiuritizacijos pakeitimas naudojant slaptažodžius ar kitas autentifikavimo priemones
MM9	**Duomenų valdymas**	Įprastinių duomenų atsarginių kopijų rengimas ir taikyti tinkamo duomenų apdorojimo įmonėje metodus pagal BDAR.
MM10	**Vaidmenimis grįstos prieigos kontrolė**	Sukūrimas administratoriaus paskyros ir apribojimas prieigos teises tarp darbuotojų, pagal jų padėtį ir pareigas įmonėje.
MM11	**Slaptažodžių valdymas**	Asmeninių darbuotojų prieigos slaptažodžių sukūrimas ir jų saugojimo ir atkūrimo proceso užtikrinimas.
MM12	**Verslo tęstinumo valdymas**	Gairių ir procedūrų, dėl nenumatytų atvejų atsiradimo parengimas.
MM13	**Mediacija ir suinteresuotųjų šalių valdymas**	Įmonės vadovų ir darbuotojų poreikių koordinavimas, teikiant informaciją ir įžvalgas abiem šalims.

6 Išsamus mokymo modulių aprašymas (vadovaujantis ECVET kriterijais)

6.1 MM1 – Procesų valdymas

Mokymų modulis 1	Procesų valdymas
Bendras aprašymas/ siekiamas rezultatas	Verslo procesų analizė ir strateginės duomenų apsaugos ir informacijos saugumo ataskaitos rengimas
Numeris	MM 1
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
Veiklos kompetencijos	Dalyviai mokosi suprasti įmonėje atliekamos struktūrinės procesų analizės svarbą. Geba atpažinti procesus, kuriuos būtina toliau analizuoti atsižvelgiant į jų poveikį duomenų ir informacijos saugumui. Susipažįsta su procesų dokumentacija ir geba stebėti darbo rutinos pokyčius. Geba parengti dokumentus, kurie leidžia formuluoti rekomendacijas dėl veiksmų.
Mokymosi rezultatai	**Techninė/ profesinė kompetencija** Mokymų dalyviai **žinos:** - kaip taikyti BDAR gaires ir gerąją informacijos saugumo praktiką. - kaip nustatyti, dokumentuoti, projektuoti, įgyvendinti, valdyti ir optimizuoti verslo procesus. - kaip strategiškai planuoti procesų dokumentaciją. - apie komunikacijos būdus ir kanalus. Mokymų dalyviai **gebės:** - įdiegti dokumentus naudojant elektroninio duomenų apdorojimo (EDA) sistemas. - apibendrinti originalią pirminę informaciją, - efektyviai bendrauti su kolegomis siekiant koreguoti darbo eigą. - tinkamai reaguoti į kitų komentarus, pvz., priimti konstruktyvią kritiką ir aktyviai klausytis, siekiant rasti geriausius sprendimus. - rasti tinkamą teisinę ir techninę informaciją bei atitinkamas rekomendacijas iš patikimų šaltinių veiksmams atlikti. **Asmeninė kompetencija** Mokymų dalyviai **gebės:** - savarankiškai organizuoti dokumentacijos procesą, dirbant struktūrizuotu būdu, daugiausia dėmesio skiriant detalėms. - savarankiškai bendrauti su kolegomis, bendravimą grindžiant pasitikėjimu.

	- suprasti su užduotimi susijusią atsakomybę ir atsakomybę ir pasitikėti savimi bendraujant su kitais. -
Rekomendacijos mokymui ir mokymuisi	Procesų dokumentacija grįsta praktiniais pavyzdžiais . EDA sistemos dokumentacijos veiklos laisva forma ir naudojant tekstinius modulius.
Literatūra ir papildomi ištekliai mokymuisi	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]. Available: https://eugdpr.org. General data protection regulation (2018). Official Journal of the European Union [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:32016R0679. Gellert, R. (2015). Understanding data protection as risk regulation. *Journal of Internet Law*, 18 (11), 3-15.

6.2 MM2 - IKT rizikos valdymas

Mokymų modulis 2	IKT rizikos valdymas
Bendras aprašymas/ siekiamas rezultatas	**Įmonės pokyčių, kurie turi įtakos įmonės saugumo strategijai stebėsena ir ataskaitos kolegoms rengimas**
Numeris	MM 2
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
Veiklos kompetencijos	Dalyviai mokosi suprasti technologinių pokyčių dinamiką ir jų įtaką įmonės strategijai siekiant sumažinti riziką. Geba nuspręsti, kaip skubiai reaguoti į šią riziką. Gebės sekti technologinius pokyčius įmonėje ir už jos ribų bei pateikti įmonės rizikos poveikio vertinimus.
Mokymosi rezultatai	**Techninė/ profesinė kompetencija** Mokymų dalyviai **žinos:** - apie įmonės patiriamos rizikos vertinimą ir esamų priemonių tinkamumą rizikai įveikti. - kaip stebėti technologinius pokyčius įmonėje ir už jos ribų, taip pat personalo pokyčius. - kaip nustatyti tvarkomų asmens duomenų kiekį ir paskirtį. Mokymų dalyviai **gebės:** - rasti informacijos apie technologijų plėtrą, vadovaujantis informacijos šaltiniais, gautais iš valstybinių ar privačių šios srities institucijų. - aptikti riziką, nepaisant teorinio darbuotojų nenoro atskleisti klaidas ar trūkumus. - remiantis gauta informacija teikti rekomendacijas dėl veiksmų. - įvertinti ir sumažinti su duomenų apsauga susijusią riziką. - nustatyti asmens duomenų saugyklas / tvarkymo operacijas organizacijose ir įvertinti jų kontekstą. - imtis strateginių veiksmų, siekiant sutelkti išteklius ir darbuotojus bendradarbiavimui stiprinti. - demonstruoti atsparumą, kai susiduria su kolegų nenoru bendradarbiauti. **Asmeninė kompetencija** **Mokymų dalyviai gebės:** - demonstruoti atsparumą, kai susiduria su kolegų nenoru bendradarbiauti. - išlikti lanksčiais siekiant rasti sprendimus ir sukurti palankią aplinką. - strategiškai ir organizuotai atlikti užduotis.
Rekomendacijos mokymui ir mokymuisi	Procesų dokumentacija su realiais pavyzdžiais. EDA sistemos dokumentacijos veiklos laisva forma ir naudojant tekstinius modulius.

Literatūra ir papildomi ištekliai mokymuisi	European Banking Authority (2019). Final Report: EBA Guidelines on ICT and security risk management [Online]. Available: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020. NZ Digital Government (2021). ICT Risk Management Guidance [Online]. Available: www.digital.govt.nz/dmsdocument/130-ict-risk-management-guidance/html. Commission de Surveillance du Secteur Financier (CSSF) (2020). ICT Risk [Online]. Available: 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.

6.3 MM3 – Atitikties valdymas

Mokymų modulis 3	Atitikties valdymas
Bendras aprašymas/ siekiamas rezultatas	**Įmonės gairių, kaip elgtis su konkrečia informacija ir duomenimis parengimas**
Numeris	MM 3
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
Veiklos kompetencijos	Dalyviai supras, kaip svarbu kodifikuoti įmonės elgesio gaires, kad būtų galima tinkamai elgtis su duomenimis ir informacija. Sužinos, kaip nustatyti gaires, kurios užtikrintų, kad darbuotojai laikytųsi reikalavimų. Supras, kaip svarbu pasirengti numatytiems ir nenumatytiems atvejams ir nustatyti visos įmonės taisykles, kaip elgtis ir kokių priemonių imtis kritinėse situacijose.
Mokymosi rezultatai	**Techninė/ profesinė kompetencija** Mokymų dalyviai **žinos:** - apie BDAR reglamentavimą ir nacionalinius teisės aktus, reglamentuojančius informacijos saugumą ir duomenų apsaugą. - apie informacijos architektūrą ir organizacijos vidaus komunikacijos kanalus - kaip išanalizuoti, aprašyti ir dokumentuoti procesus, dėl kurių gali kilti galimas konfliktas su atitikties politika. - kaip parengti atitikties politikos gaires. - kaip rinkti, tvarkyti ir vertinti duomenų tvarkymo techniką. - kaip analitiškai mąstyti apdorojant kondensuotą informaciją, kuriant sprendimus ir priimant su atitikties valdymu susijusius sprendimus. Mokymų dalyviai **gebės:** - įgyvendinti teisiniuose dokumentuose aprašytas procedūras. - nustatyti ypatingos svarbos duomenų ir informacijos vienetus, kuriuos reikia ypatingai saugoti ar tvarkyti. - analizuoti ir sudaryti su informacijos srautu susijusių procesų organizacijoje žemėlapį. - atpažinti galimus pavojus ir grėsmes informacijos saugumui ir duomenų apsaugai organizacijos vidaus procesuose. - rengti su atitikties valdymu susijusius praktinių, operatyvinių ar konceptualių problemų sprendimus, susijusius su įvairiomis kasdienio darbo užduotimis. - suprasti atitikties politikos gairių paskirtį ir jas atnaujinti kritiniais atvejais. - taikyti analitinio ir kritinio mąstymo įgūdžius nustatant galimų su atitikties valdymu susijusių problemų sprendimų privalumus ir trūkumus. - patogiai ir prasmingai apibendrinti informaciją. **Asmeninė kompetencija**

	Mokymų dalyviai gebės: - dirbti struktūrizuotai, daugiausia dėmesio skiriant detalėms. - atpažinti su užduotimis susijusią atsakomybę ir pasitikėti savimi bendraujant su kitais. - savarankiškai atlikti užduotis ir parodyti norą mokytis.. -
Rekomendacijos mokymui ir mokymuisi	Procesų dokumentacija su realiais pavyzdžiais. EDA sistemos dokumentacijos veiklos laisva forma ir naudojant tekstinius modulius.
Literatūra ir papildomi ištekliai mokymuisi	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]. Available: 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]. Available: 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). Using Models to Enable Compliance Checking Against the 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 as Support for Implementation of Regulations: Approach and Experiences from

	GDPR. Complex Systems Informatics and Modeling Quarterly, (24), 31-48.

6.4 MM4 – IKT viešieji pirkimai

Mokymų modulis 4	IKT viešieji pirkimai
Bendras aprašymas/ siekiamas rezultatas	**Rekomendacijų dėl įsigyjamų daiktų parengimas, atsižvelgiant į įmonės informacijos saugumo ir duomenų apsaugos reikalavimus.**
Numeris	MM 4
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
Veiklos kompetencijos	Dalyviai supras viešųjų pirkimų svarbą informacijos saugumo ir duomenų apsaugos įgyvendinimui. Žinos, kaip pozicionuoti savo kompetenciją įmonės viešųjų pirkimų procese. Gebės daryti įtaką naujų technologijų ir technikos pirkimui bei įvertinti jų tinkamumą naudoti, atsižvelgiant į įmonės duomenų apsaugos ir informacijos saugumo gaires.
Mokymosi rezultatai	**Techninė/ profesinė kompetencija** Mokymų dalyviai **žinos:** - apie įmonės saugumo ir specifikacijos reikalavimus, susijusius su nauja įranga. - apie esamos techninės įrangos specifikacijas ir būtinybę jas skubiai pakeisti naujomis technologijomis. - apie paslaugų teikėjų ir įrangos apgaulę dėl BDAR pažeidimų. Mokymų dalyviai **gebės:** -parengti ir pristatyti trumpą pristatymą (reportažą, procedūrą, procesą, strategiją), skirtą technologijai ar technikai, kurią reikia įsigyti, įvertinti. - perduoti informaciją iš įvairių darbuotojų, skyrių apie jų poreikius ir pateikti rekomendaciją dėl įsigijimo. - surinkti išsamią informaciją apie perkamą technologiją, mašinas. - surasti atitinkamą teisinę ir techninę informaciją ir, remdamiesi šia užklausa, priimti sprendimus. - imtis veiksmų, susijusių su strateginiu lygmeniu nustatytais tikslais ir procedūromis, siekiant sutelkti išteklius ir įgyvendinti nustatytas strategijas. - planuoti ir valdyti išteklius, atsižvelgiant į biudžeto ir laiko apribojimus, ir siekti nustatytų tikslų, naudojantis projekto eigos stebėjimo ir kokybės kontrolės priemonėmis. **Asmeninė kompetencija** **Mokymų dalyviai gebės:** - sužinoti apie rinkoje egzistuojantį įmonės problemos sprendimą. - skirti dėmesio detalėms (teisinėms ir techninėms). - rodyti pasitikėjimą ir atsakomybę bendraujant su suinteresuotomis šalimis.

Rekomendacijos mokymui ir mokymuisi	Procesų dokumentacija su realiais pavyzdžiais. EDA sistemos dokumentacijos veiklos laisva forma ir naudojant tekstinius modulius.
Literatūra ir papildomi ištekliai mokymuisi	Australian Government: Digital Transformation Agency (2021). ICT procurement [Online]. Available: www.dta.gov.au/help-and-advice/ict-procurement. Moses, M. (2019). Procurement Process and ICT. Zerite Network [Online]. Available: http://zeritenetwork.com/procurement-process-and-ict/. European Commission (2016). Best practices for ICT procurement based on standards in order to promote efficiency and reduce lock-in: 2-year project completed [Online]. Available: ec.europa.eu/digital-single-market/en/news/. Dovgalenko, S. (2020). The Technology Procurement Handbook: A Practical Guide to Digital Buying. London: Kogan Page.

6.5 MM5 – Sensityvumas ir įtaka

Mokymų modulis 5	Sensityvumas ir įtaka
Bendras aprašymas/ siekiamas rezultatas	**Veiklų (Informavimo) vykdymas, siekiant atkreipti darbuotojų dėmesį į saugumo rizikas ir sužadinant darbuotojų sąmoningumą.**
Numeris	MM 5
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
Veiklos kompetencijos	Mokymų dalyviai supras, kaip svarbu informuoti darbuotojus ir įmonės vadovus apie duomenų apsaugos ir informacijos saugumo problemas. Išmoks skleisti informaciją apie dažniausiai pasitaikančias grėsmes ir ugdyti darbuotojų gebėjimus aptikti tikėtinas grėsmes jų kasdienėje profesinėje veikloje. Gebės atlikti informuotumo lygio įmonėje analizę ir įgyvendinti atitinkamas informuotumo didinimo priemones.
Mokymosi rezultatai	**Techninė/ profesinė kompetencija** Mokymų dalyviai **žinos:** - apie pagrindines BDAR gaires. - kaip elgtis su galimais procesais ir darbuotojais, kurie gali būti pažeidžiami dėl atakų ar neskelbtinos informacijos bei duomenų praradimo. - kaip galima įgyvendinti audito priemones - apie komunikacijos būdus ir kanalus - kaip įgyvendinti pokyčių strategijas Mokymų dalyviai **gebės:** - rasti tinkamą teisinių žinių šaltinį. - bendradarbiauti su kitais asmenimis, siekiant nustatyti pokyčių poreikį ir juos įgyvendinti - veiksmingai bendrauti su kitais, pasirenkant ne tik pranešimo tipą, bet ir jo apimtį bei svarbą atsižvelgiant į aplinkybes. **Asmeninė kompetencija** Mokymų dalyviai **gebės:** - prisitaikyti prie besikeičiančių sąlygų ir aplinkybių, dirbant organizuotai ir išlaikant atstumą, leidžiantį tinkamai save įvertinti. - būti pavyzdžiu kitiems darbuotojams, laikytis profesinės etikos kodekso ir demonstruoti atsakomybę.
Rekomendacijos mokymui ir mokymuisi	Iliustruokite teoriją praktiniais pavyzdžiais, pvz., pasitikrinimo priemonėmis ir atvejų analize. Galimų praktinių atvejų pavydžiai: - suklastotos USB atmintinės, - žmogaus inžinerijos atvejai, - suklastotų elektroninių laiškų siuntimas.

	Taikykite interaktyvius mokymo metodus (pvz., darbas grupėse, diskusijos, atvejų analizė, simuliaciniai vaidmenų žaidimai ir kt.)
Literatūra ir papildomi ištekliai mokymuisi	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 awareness: a matter of people, culture, leadership and acting now [Online]. Available: 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]. Available: 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]. Available: www.enisa.europa.eu General Data Protection Regulation (2021). Complete guide to GDPR compliance [Online]. Available: https://gdpr.eu/

6.6 MM6 – Švietimas ir mokymas

Mokymų modulis 6	Švietimas ir mokymas
Bendras aprašymas/ siekiamas rezultatas	**Įmonės mokymo planų parengimas, siekiant vykdyti reguliarius darbuotojų mokymus informacijos saugumo ir duomenų apsaugos srityse.**
Numeris	MM 6
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
Veiklos kompetencijos	Mokymų dalyviai supras švietimo svarbą duomenų apsaugos ir informacijos saugumo srityje. Mokės mokytis ir mokyti kitus įmonės darbuotojus. Gebės konsultuodamiesi ir bendraudami su darbuotojais išsiaiškinti jų mokymo(si) poreikius. Išmoks rengti mokymo medžiagą ir mokyti darbuotojus į savo kasdienę profesinę veiklą įtraukti tinkamas darbo procedūras.
Mokymosi rezultatai	**Techninė/ profesinė kompetencija** Mokymų dalyviai **žinos:** - kur rasti nacionalinius teisinius dokumentus, reglamentuojančius informacijos saugumą ir duomenų apsaugą (BDAR pagrindai). - kaip parengti mokymų medžiagą ir kaip vykdyti mokymus, kad į juos būtų įtraukta tinkama darbo tvarka. - kaip individualiai konsultuoti darbuotojus Mokymų dalyviai **gebės**: - supažindinti darbuotojus, kaip praktiškai taikyti nacionalinius teisinius dokumentus informacijos saugumo ir duomenų apsaugos srityje, vadovaujantis BDAR gairėmis. - ugdyti darbuotojų nuostatas sąmoningai ir nuolatos tobulėti abiejose srityse. - teikti pagalbą ir individualiai konsultuoti darbuotojus dėl nustatytų mokymų poreikio. - rengti praktinių, veiklos ar konceptualių problemų, kylančių atliekant darbą įvairiuose kontekstuose, sprendimus. **Asmeninė kompetencija** **Mokymų dalyviai gebės:** - savarankiškai organizuoti mokymus įmonėje, atsižvelgiant į nustatytus darbuotojų poreikius. - savarankiškai bendrauti su kolegomis ir užmezgant pasitikėjimu grįstą santykį.. - pripažinti su užduotimis susijusią atsakomybę ir motyvuoti darbuotojus mokytis. -

Rekomendacijos mokymui ir mokymuisi	Informacijos saugumo ir duomenų apsaugos sunkumų, su kuriais susiduriama kasdieniame darbe, dokumentavimas, siekiant suplanuoti ir įgyvendinti tinkamas mokymo priemones.
Literatūra ir papildomi ištekliai mokymuisi	Pipkin, D. (2000). Information security: Protecting the global enterprise. New York: Hewlett-Packard Company. Da Veiga, A., Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. 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 Benefits of Security Awareness Training [Online]. Available: https://resources.infosecinstitute.com/topic/10-benefits-of-security-awareness-training/. GDPR informer (2017). Data Protection Training: 10 Tips for Your Staff [Online]. Available: https://gdprinformer.com/gdpr-articles/data-protection-training-10-tips-staff.

6.7 MM7 – Saugumo testavimas

Mokymų modulis 7	Saugumo testavimas
Bendras aprašymas/ siekiamas rezultatas	**Antivirusinės programinę įrangos ir užkardos įdiegimas. Atnaujinimų atlikimas ir pagrindinių metodų pritaikymas, užtikrinant įmonėje naudojamos programinės įrangos saugumą ir atitinkamų dokumentų pateikimą.**
Numeris	MM 7
Tipas	Privalomas – turi būti apibrėžtas
Apimtis	Valandos - turi būti apibrėžtos
Veiklos kompetencijos	Dalyviai supras esamos IKT infrastruktūros pažeidžiamumo, atsižvelgiant į technologijų plėtrą, patikrinimo svarbą. Išmoks naudotis (arba su išorės pagalba suprasti) įsiskverbimo testavimo priemonėmis, kad užtikrintų ugniasienių (firewalls) ir ryšių kanalų saugumą. Yra begalė būdų, kaip įsilaužti į programą. Ir saugumo testavimas pats savaime nėra vienintelis (ar geriausias) rodiklis, parodantis, kiek saugi yra programa. Tačiau labai rekomenduojama, kad saugumo testavimas būtų įtrauktas į standartinį programinės įrangos kūrimo procesą.
Mokymosi rezultatai	**Techninė/ profesinė kompetencija** Mokymų dalyviai **žinos**: - apie tinklo saugumą: tai reiškia, kad reikia ieškoti pažeidimų tinklo infrastruktūroje (ištekliuose ir politikoje). - apie sistemos programinės įrangos saugumą: tai apima įvairios programinės įrangos (operacinės sistemos, duomenų bazių sistemos ir kitos programinės įrangos), nuo kurios priklauso taikomoji programa, silpnųjų vietų vertinimą. - apie kliento programinės įrangos saugumą: tai susiję su kliento (naršyklės ar kitos panašios priemonės) apsaugos nuo manipuliacijų užtikrinimu. - apie serverio saugumą: Tai susiję su užtikrinimu, kad serverio kodas ir jo technologijos būtų pakankamai patikimos ir apsaugotų nuo bet kokio įsilaužimo. Mokymų dalyviai įgis **gebės**: - kurti testus, skirtus programinės įrangos saugumui nustatyti. - pritaikyti esamą sistemą. - prisijungti prie kompiuterių sistemos ar tinklo turint leidimą. - užtikrinti sistemas, kad nebūtų duomenų vagystės ar sunaikinimo. - atlikti didžiąją dalį nutraukimo veiklos gavus vadovo leidimą. **Asmeninė kompetencija** **Mokymų dalyviai gebės:** - pripažinti, kad procesų dokumentavimas yra atspirties taškas tolesniems darbo veiksmams. - dirbti struktūruotai, daugiausia dėmesio skiriant detalėms.

	- pripažinti atsakomybę, susijusią su užduotimi, ir pasitikėti savimi bendraujant su kitais.
Rekomendacijos mokymui ir mokymuisi	Dauguma saugumo testavimo tipų apima sudėtingus veiksmus ir nestandartinį mąstymą, tačiau kartais reikia atlikti paprastus testus, kurie padeda atskleisti rimčiausius saugumo pavojus.
Literatūra ir papildomi ištekliai mokymuisi	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.

6.8 MM8 – Kodavimas

Mokymų modulis 8	Kodavimas
General Description / Output	**Work on securitisation of mobile devices, communication channels and data storage units via passwords or other means of authentication.**
Code number	LU 8
Type	Mandatory – to be defined
Volume	Hours - to be defined
Action Competences	The participants learn to understand the importance of password encoding for their vulnerability in the face of technological developments. They learn to use (or understand with an external support) password encoding tools to ensure the security of firewalls and communication channels. Password Encoding is the process in which a password is converted from a literal text format into a humanly unreadable sequence of characters. If done correctly, it is very difficult to revert back to the original password and so it helps secure user credentials and prevent unauthorized access to a website.
Learning Outcomes	**Technical Competence** The participants **Know** - about Literal Values: Passwords were stored in literal text format in databases without any encoding or hashing. As databases need authentication, which nobody except the admins and the application had, this was considered safe. - about Encryption: It is a safer alternative and the first step taken towards password security. - about Hashing: To combat these attacks, developers had to come up with a way to protect passwords in a database in such a way that they cannot be decrypted. - about Salting: To combat the appearance of rainbow tables, developers started adding a random sequence of characters to the beginnings of the hashed passwords. - about Password Encoders: It provides multiple password encoding implementations to choose from. Each have their advantages and disadvantages, and a developer can choose which one to use depending on the authentication requirement of their application. **Can** - educate the team on password encoding best practice. - educate the team on cyber security. - decide what password types not to use. - define the right way to generate encoding processes. - eliminate complex passwords.

	- strongly reduce the risk of copying a password. - ensure password auditing and accountability. **Personal Competence** **The participants are able to** - recognize the documentation of processes as a starting point for further working steps. - work in a structured way with a focus on details. - recognize the responsibility belonging to the task and be confident in the interaction with others. - manage the main requested tasks with a good level of autonomy. - emphasise their social competences (soft skills, empathy and communication in particular).
Recommendations for Learning & Teaching	Most types of encoding processes involve complex steps and out-of-the-box thinking but, sometimes, it is simple tests like the one above that help expose the most severe encoding risks.
Literature & Further Resources	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 and the Text Encoding Initiative Schema. Journal of the Text Encoding Initiative, (8), 1-16. doi: 10.4000/jtei.1054.

6.9 MM9 - Duomenų valdymas

Mokymų modulis 9	Duomenų valdymas
Bendras aprašymas / Rezultatai	**Atlikti įprastines atsargines duomenų kopijas ir laikytis BDAR reikalavimų apdorojant duomenis įmonėje.**
Kodo numeris	MD 9
Tipas	Privaloma nurodyti
Apimtis	Nurodyti valandų skaičių
Veiklos kompetencijos	Dalyviai mokosi suprasti duomenų ir informacijos saugojimo bei apdorojimo pagal numatytas gaires svarbą. Jie išmoksta kaip tinkamai elgtis su duomenimis laikantis BDAR reikalavimų. Dalyviai gali įvertinti fizinių ir elektroninių duomenų saugojimą ir apdorojimą įmonėje bei nustatyti galimą netinkamą elgesį. Siekiant sušvelninti šią riziką dalyviai išmoks pasiūlyti pakeitimus įmonės procesuose.
Mokymosi rezultatai	**Techninės kompetencijos** Dalyviai **Žino** - kaip apibrėžti sėkmingam procesui reikalingus informacijos poreikius: kokie duomenys yra tvarkomi organizacijoje ir kokie saugojimo būdai turėtų atitikti esamas taisykles. - taisykles, kaip nustatyti asmens duomenų saugojimo ir apdorojimo operacijų apimtį ir tikslą. - kaip organizuoti ir taikyti duomenų valdymą įmonėje: prisitaikyti prie pokyčių, taikyti analitinį mąstymą, kurti sprendimus; savarankiškai atlikti projekto valdymo užduotis. - įvairius būdus ir bendravimo stilius, siekiant gauti reikiamos informacijos apie saugojimą. **Geba** - nustatyti organizacijoje saugomų / tvarkomų asmens duomenų apimtį ir paskirtį. - reguliariai kurti atsargines duomenų kopijas siekiant sumažinti riziką prarasti vertingus duomenis ir informaciją. - dirbti grupėje, siekiant efektyvaus procesų pagerinimo. - siekiant konkretaus tikslo planuoti ir valdyti įvairius išteklius bei stebėti duomenų valdymo procesą. **Asmeninės kompetencijos** **Dalyviai gali** - dirbti struktūrizuotai, daug dėmesio skiriant detalėms. - atpažinti su užduotimis susijusias atsakomybes ir pasitikėti savimi bendraujant su kitais. - savarankiškai atlikti užduotis ir noriai mokytis.

Mokymosi ir mokymo rekomendacijos	Susiekite teorines žinias su praktiniais pavyzdžiais. Taikykite interaktyvius mokymo metodus (pvz., grupinį darbą, diskusijas, atvejų analizę, vaidmenų modeliavimą ir t. t.)
Literatūra ir kiti šaltiniai	Calabro, A., Daoudagh, S., & Marchetti, E. (2020). Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. Information Systems (91) [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306437919305216. Guide on Good Data Protection Practice in Research (2019) [Online]. Available: https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf. EU-GDPR. (2019). EU GDPR portal. [Online]. Available: https://eugdpr.org. General data protection regulation (2018). Official Journal of the European Union [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

6.10 MM10 - Vaidmenimis grįstos prieigos kontrolė

Mokymų modulis 10	Vaidmenimis grįstos prieigos kontrolė
Bendras aprašymas / Rezultatai	**Sukurti administratoriaus paskyras ir apriboti darbuotojų prieigos teises atsižvelgiant į nustatytus apsaugos lygius.**
Kodo numeris	MD 10
Tipas	Privaloma nurodyti
Apimtis	Nurodyti valandų skaičių
Veiklos kompetencijos	Dalyviai mokosi suprasti, kaip svarbu, esant galimybėms, apriboti prieigą prie duomenų, informacijos ar fizinės infrastruktūros ir suteikti prieigą tik tam tikrai darbuotojų grupei. Jie išmoksta kaip nustatyti tinkamus apribojimus atsižvelgiant į nustatytą saugumo lygį. Dalyviai gebės priskirti tinkamus vaidmenis įmonėje prie saugumo prieigos lygių ir prireikus sukurti prieigą prie konkrečios atsekamos informacijos.
Mokymosi rezultatai	**Techninė kompetencija** Dalyviai **Žino** - kaip nustatyti organizacijoje atliekamas pagrindines su asmens duomenims susijusias operacijas. - kaip nustatyti informacijos prieinamumą konkrečioms darbuotojų grupėms. - kaip, esant reikalui, nustatyti tinkamus apribojimus atsižvelgiant į apibrėžtus ir sulygtus saugumo lygius. **Geba** - išskirti atskirų darbuotojų ir grupių vaidmenis, siekiant nustatyti jų poreikius įvairiems saugumo lygiams (remiantis vadovybės patvirtintais priskirtais saugumo lygiais). - rasti tinkamus sprendimus atskiriems darbuotojams ar jų grupėms leidžiančius ar ribojančius tam tikrą prieigą ir geba juos pagrįsti. - valdyti individualias vartotojo teises priskiriant tinkamas roles vartotojo paskyrai, kai šios rolės yra apibrėžtos vadovybės. **Asmeninės kompetencijos** **Dalyviai gali** - savarankiškai paskirti atitinkamas roles pagal vadovybės reikalavimus (priskirtus saugumo lygius). - savarankiškai ir su pasitikėjimu bendrauti su kolegomis ir vadovybe.

	- Savarankiškai atpažinti atsakomybes susietas su užduotimi gerbiant kitų poreikius.
Mokymosi ir mokymo rekomendacijos	Sužinokite / mokykite apie tris pagrindines taisykles, apibrėžtas rolėmis grįstame prieigos valdyme (RBAC): 1) vaidmens priskyrimas, 2) vaidmens teisių suteikimas, 3) leidimo suteikimas. Pagalvokite apie jautrumo svarbą priskiriant vaidmenį ir tai aiškiai aptarkite su vadovybe.
Literatūra ir kiti šaltiniai	Blokdyk, G., (2017). Role-based Access Control: A Successful Design Process. D Ferraiolo, DR Kuhn, R Chandramouli, (2003), Role-based access control. Benantar, M., (2006)., Access Control Systems: Security, Identity Management and Trust Models. New York: Springer. Zhang, E. (2020). What is Role-Based Access Control (RBAC)? Examples, Benefits, and More [Online]. Available: https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more.

6.11 MM11 – Slaptažodžių valdymas

Mokymų modulis 11	Slaptažodžių valdymas
Bendras aprašymas / Rezultatas	**Sukurti atskirų darbuotojų prieigos slaptažodžius ir užtikrinti saugų saugojimo ir atkūrimo procesą.**
Kodo numeris	MD 11
Tipas	Privaloma nurodyti
Apimtis	Nurodyti valandų skaičių
Veiklos kompetencijos	Dalyviai mokosi suprasti kaip svarbu centralizuoti slaptažodžių naudojimo valdymą įmonėje. Jie sužinos, kaip nustatyti slaptažodžius, užtikrinančius autentifikavimą (tarp darbuotojų) ir kaip atstatyti slaptažodžius. Dalyviai mokosi struktūriškai kurti, naudoti / valdyti, saugoti ir pakeisti darbuotojų slaptažodžius.
Mokymosi rezultatai	**Techninės kompetencijos** Dalyviai **Žino** - apie slaptažodžių saugojimą. - apie slaptažodžio perdavimą. - apie slaptažodžio spėjimą. - apie slaptažodžių atskleidimą. - apie slaptažodžio pakeitimą. **Geba** - supažinti komandą su geriausiomis slaptažodžių praktikomis. - supažindinti komandą su kibernetinio saugumo klausimais. - nuspręsti, kokių slaptažodžių tipų nenaudoti. - sukurti sudėtingus slaptažodžius. - panaudoti automatizavimo pajėgumus. - pašalinti sudėtingus slaptažodžius. - pašalinti slaptažodžio atkūrimo poreikį. - užtikrinti slaptažodžių auditą ir atskaitomybę. **Asmeninės kompetencijos** **Dalyviai gali** - atpažinti procesų dokumentaciją kaip atskaitos tašką tolesniems darbo etapams. - dirbti struktūrizuotai, daug dėmesio skiriant detalėms. - atpažinti su užduotimis susijusias atsakomybes ir pasitikėti savimi bendraujant su kitais. - savarankiškai vykdyti pagrindines prašomas užduotis. - pabrėžti savo socialines kompetencijas (ypač minkštus įgūdžius, empatiją ir bendravimą).

Mokymosi ir mokymo rekomendacijos	Slaptažodžių valdymas naudojant realius pavyzdžius. Laisvos formos dokumentacijos pratimai su teksto modulių pagalba.
Literatūra ir kiti šaltiniai	Luca, M. (2008). Password Management for Distributed Environments. Saarbrücken: VDM Verlag Dr. Müller. Smith, S. B. (2017). Password Manager: Keep Record of Internet User ID and Passwords in the Password Manage. Keep your internet login info in a safe offline location. CreateSpace: North Charleston.

6.12 MM12 - Verslo tęstinumo valdymas

Learning Unit 12	Business Continuity Management
Bendras aprašymas / Rezultatas	**Gairių ir procedūrų, dėl nenumatytų atvejų atsiradimo parengimas.**
Kodo numeris	MD 12
Tipas	Privaloma nurodyti
Apimtis	Nurodyti valandų skaičių
Veiklos kompetencijos	Dalyviai išmoks suprasti scenarijų „kas būtų, jei būtų“ svarbą. Jie mokosi analizuoti teorinius nenumatytus atvejus ir atsižvelgiant į tai parengti strategines gaires. Dalyviai galės nustatyti gaires ir iš anksto numatyti priemones, kad esant reikalui būtų pasirengę ir koordinuotai reaguotų į iškilusias naujas situacijas. -
Mokymosi rezultatai	**Techninės kompetencijos** Dalyviai **Žino** - kaip rasti nacionalinius dokumentus ir kaip ieškoti informacijos nacionaliniuose teisiniuose dokumentuose, reglamentuojančiuose saugumą ir duomenų apsaugą. - simuliacijos metodus skirtus galimiems duomenų pažeidimams numatyti. - kaip elgtis su rizikos vertinimo taisyklėmis. **Geba** - nustatyti rizikas naudojant skirtingas technikas ir bendravimo stilius. - įgyvendinti rizikos vertinimo taisykles pritariant vadovybei. - planuoti ir kurti sprendimus, prisitaikant prie organizacijoje esančių aplinkybių ir pokyčių, ir juos įgyvendinti vadovybei pritarus. - rasti naujų sprendimų, pagrįstų ankstesnių įvykių analize. **Asmeninės kompetencijos** **Dalyviai gali** - dirbti nepalankiomis sąlygomis išlaikant dėmesį detalėms. - lengvai prisitaikyti prie naujų aplinkybių.

	- būti pavyzdžiu kitiems darbuotojams laikantis jų etikos elgesio kodekso ir parodyti atsakomybę.
Mokymosi ir mokymo rekomendacijos	Teorinė skirtingų grėsmių ir rizikos situacijų scenarijų praktika. Darbas su realių situacijų pavyzdžiais.

6.13 MM13 – Mediacija ir suinteresuotųjų šalių valdymas

Mokymų modulis 13	Mediacija ir suinteresuotųjų šalių valdymas
Bendras aprašymas / Rezultatas	**Įmonės vadovų ir darbuotojų poreikių koordinavimas, teikiant informaciją ir įžvalgas abiem šalims.**
Kodo numeris	MD 13
Tipas	Privaloma nurodyti
Volume Apimtis	Nurodyti valandų skaičių
Veiklos kompetencijos	Dalyviai mokosi suprasti koordinavimo su visais įmonės suinteresuotais asmenimis svarbą atsižvelgiant į jų vaidmenį ir įtaką susijusią su duomenų apsauga ir informacijos saugumu. Jie išmoksta efektyviai bendrauti su skirtingais hierarchijos lygmenimis (darbuotojais ir vadovybe) ir pasikeitus organizacinei tvarkai pritaikyti prie jos savo poreikius bei interesus. Dalyviai gebės diplomatiškai bendrauti su suinteresuotosiomis šalimis ir susidoroti su galimu pasipriešinimu savo įtakai.
Mokymosi rezultatai	**Techninės kompetencijos** Dalyviai **Žino** - kaip rasti nacionalinius teisinius dokumentus, reglamentuojančius informacijos saugumą ir duomenų apsaugą, ir kaip ieškoti informacijos. - kokie vidiniai ir išoriniai komunikacijos kanalai gali būti naudojami vadovybei pritarus, ir kokia yra su jais susijusi rizika. - kokios priemonės gali būti taikomos norint stebėti, išbandyti ir įvertinti procesus organizacijoje. - kokios priemonės gali būti taikomos rizikai įvertinti ir kaip elgtis vertinant riziką. **Geba** - įgyvendinti vidaus audito priemones (vadovybei pritarus). - planuoti ir plėtoti strateginius sprendimus bei juos įgyvendinti gavus vadovybės pritarimą. - vadovybei pritariant įdiegti prevencinę kultūrą. - nustatyti, įvertinti ir prioretizuoti rizikas. - sukurti vidaus taisykles visai organizacijai ir jas įgyvendinti (vadovybei patvirtinus). **Asmeninės kompetencijos** **Dalyviai gali**

	- susidoroti su pokyčiais ir prisitaikyti. - būti kūrybiški ir siekti tolesnio tobulėjimo. - remtis savo etikos kodeksu, kad kiti galėtų vadovautis jų pavyzdžiu. -
Mokymosi ir mokymo rekomendacijos	Susiekite teorines žinias su praktiniais pavyzdžiais. Taikykite interaktyvius mokymo metodus (pvz., darbas grupėse, diskusijos, atvejų analizė, vaidmenų modeliavimas ir t. t.)
Literatūra ir kiti šaltiniai	IT Governance Privacy Team (2020). EU General Data Protection Regulation (GDPR) – An implementation and compliance guide (4th ed.). General data protection regulation (2021). Complete guide to GDPR compliance [Online]. Available: https://gdpr.eu/. Gorondutse, A. H., & Hilman, H. (2016). Mediation effect of organizational culture on the relationship between perceived ethics and SMEs. Journal of Industrial Engineering and Management 2016, 9(2), 505-529. Straight, J. (2018). GDPR compliance: Identifying an organization's unique profile [Online]. Available: https://www.helpnetsecurity.com/2018/05/14/gdpr-compliance-profile/