Co-funded by the Erasmus+ Programme of the European Union

Module de instruire InCyT

Securitatea informațiilor pentru manageri Unitatea 1 Săptămâna 2 Denumirea unității: Introducere în Securitatea Informației, sisteme de control intern	
Activități de învățare	❑ **Webinar** ❑ **Exerciții** ❑ **Workshop** ❑ **Prezentare** ❑ **Alte**
Responsabil de învățare	• Gabriel Vladut • Valentin Istratie
Obiectivele activității de învățare	1. Introducere despre proiectul Erasmus+ InCyT 2. Securitate cibernetică 3. Concepte, definiții și termeni 4. Standard de control intern 5. Elaborarea controalelor de securitate cibernetică
Abilități de dobândit	• TS3 Securitatea retelei • TS4 Testare de penetrare (vulnerabilități exploatabile). • SS3 Analiza cognitivă și comportamentală
Durata activității de învățare	2 săptămâni
Cerințe de învățare	***Ce e necesar?***
	• Obțineți conștientizarea securității cibernetice și aflați ce este un atac de securitate cibernetică • Învățați metode de prevenire a încălcării datelor utilizate de atacatori pentru a accesa date sensibile și pentru a exploata vulnerabilitățile organizaționale • Aflați cum să procedați în cazul unui atac de securitate cibernetică

Co-funded by the
Erasmus+ Programme
of the European Union

Informații scurte despre modul

Descriere
Securitatea informațiilor, sistemele de control intern sunt importante și foarte adesea amenință la adresa securității cibernetice Protecția informațiilor și a sistemelor informaționale împotriva accesului sau modificării neautorizate a informațiilor, fie în stocare, procesare sau tranzit, și împotriva refuzului serviciului către utilizatorii autorizați. Securitatea informațiilor include acele măsuri necesare pentru a detecta, documenta și contracara astfel de amenințări. Securitatea informației este compusă din securitatea computerelor și securitatea comunicațiilor. Denumit și INFOSEC. Vezi și securitatea comunicațiilor; Securitatea calculatorului; securitatea informațiilor; Sistem informatic. Controalele interne sunt utilizate de către echipele de management, securitate IT, financiară, contabilă și operațională pentru a atinge următoarele obiective: 1. Asigurarea fiabilității și acurateții informațiilor financiare – Controalele interne asigură că informațiile exacte, actualizate și complete sunt reflectate în contabilitate. sisteme și rapoarte financiare. Cursanții ar putea fi informați despre astfel de aspecte citind textul corespunzător, urmărind webinarii în flux și rezolvând exerciții în ritm propriu. Toate aceste documente se află pe platforma digitală interactivă a proiectelor. Cursanții își pot testa răspunsurile prin exerciții de autoevaluare. Răspunsurile la alte exerciții ar trebui salvate pe forumul de discuții corespunzător și discutate cu mentorul la întâlnirea comună organizată o dată pe săptămână. Cursantul poate lucra în cooperare cu ceilalți și poate îndruma în special în timpul întâlnirilor. Aceștia vor fi sprijiniți să dezvolte un portofoliu electronic important pentru reflecția și evaluarea instruirii.

Conținutul materialului de învățare

Securitatea informațiilor

Securitatea informațiilor se ocupă cu protejarea informațiilor și a sistemelor informatice împotriva accesului, utilizării, dezvăluirii, întreruperii, modificării sau distrugerii neautorizate.

ISO/IEC27002/2013 se ocupă de securitatea informațiilor prin cele trei componente principale: confidențialitate, integritate și disponibilitate. Confidențialitatea este asigurată prin criptarea informațiilor. Integritatea se realizează prin mecanisme și algoritmi de împrăștiere.

Disponibilitatea este asigurată prin consolidarea securității rețelei sau rețelelor sistemului informatic și oferirea de copii de siguranță. Securitatea informațiilor este un set de practici menite să protejeze datele.

Securitatea informațiilor nu se limitează la sisteme informatice sau informații în forma sa digitală sau electronică. Mai degrabă, se aplică tuturor aspectelor legate de siguranța, securitatea și protecția datelor sau informațiilor, indiferent de forma acestora.

Securitatea informației nu poate fi definită ca fiind sinonimă cu securitatea computerelor, securitatea sistemului și a rețelei, securitatea tehnologiei informației, sistemele informaționale sau tehnologia informației și comunicațiilor. Fiecare dintre aceste expresii se referă la un subiect diferit, chiar dacă punctul comun se referă la securitatea informației în unele dintre formele sale (aici vorbim despre versiunea sa electronică): prin urmare, toate sunt subdomenii ale securității informaționale.

În secolul 21, majoritatea organizațiilor au un sistem informatic conectat la Internet și fac schimb de informații prin intermediul acestuia. Informațiile pot fi făcute să treacă printr-o interconectare a rețelelor. În consecință, această interconectare este cu atât mai expusă riscurilor de malware din partea celor care doresc să pună mâna pe informații sensibile, acționând din interior (copierea informațiilor, utilizarea codului rău intenționat) sau din exterior.

Pentru a contracara aceste riscuri, securitatea informațiilor necesită dezvoltarea unor concepte precum etichetarea datelor, criptarea cu chei publice (PKI) și securitatea pe mai multe niveluri (MLS). Pe lângă problemele de conectare a rețelelor, este din ce în ce mai ușor să mutați cantități mari de informații (și asta într-un mod relativ greu de detectat în caz de hacking), dar și să le transportați fizic prin stick-uri USB sau carduri de memorie.

Prin urmare, sistemele informatice care conțin informații sensibile sunt proiectate din ce în ce mai mult ca un mediu System high mode, în multe cazuri sub formă de rețele separate, fără conexiune la alte rețele și fără porturi USB. Sunt acceptate în mod obișnuit trei criterii de sensibilitate a

informațiilor: Disponibilitate, Integritate și Confidențialitate. Un al patrulea este, de asemenea, folosit destul de frecvent (sub diferite denumiri): Trasabilitate, Responsabilitate, Audibilitate (cu referire la auditurile computerizate) sau Evidență. Se folosește și un al cincilea criteriu: Nerepudierea, care asigură schimbul de mesaje între expeditor și destinatar.

Atacurile cibernetice și cadrul de competențe

Un cadru de competențe este utilizat în mod regulat de companii pentru a-și înțelege cerințele bazate pe abilități, competențele necesare, abilitățile angajaților și lacunele.

Atunci când un cadru de competențe este dezvoltat ținând cont de profilul companiei și de interesele angajaților, acesta poate îmbunătăți performanța și poate oferi claritate pentru fiecare cerință individuală a rolului și poate dezvolta talentul la locul de muncă. În ultimii ani, din cauza multor atacuri cibernetice, cadrele de securitate cibernetică sunt adoptate în principal de organizații mari (afaceri, ONG-uri și alte entități) sau de actori de stat.

Un atac cibernetic de succes poate provoca daune majore afacerii unei companii. Își poate afecta rezultatul final, precum și statutul de afaceri al companiei și încrederea consumatorilor. Impactul unei breșe de securitate poate fi împărțit în trei categorii: financiar, reputațional și juridic.

Atacuri cibernetice

Atacurile cibernetice duc adesea la pierderi financiare substanțiale ca urmare a furtului de informații corporative, informații financiare (de exemplu, detalii bancare sau detalii ale cardului de plată), bani, întreruperi ale tranzacțiilor (de exemplu, incapacitatea de a tranzacționa online), pierderea afacerii sau a contractului. Companiile care au suferit o încălcare cibernetică vor cheltui, în general, bani asociați cu repararea sistemelor, rețelelor și dispozitivelor afectate.

Atacurile cibernetice pot afecta reputația unei companii și încrederea pe care clienții o au în companie. Acest lucru ar putea duce la pierderi de clienți, vânzări și profituri reduse. Efectul prejudiciului reputației poate afecta chiar furnizorii companiei sau poate afecta relațiile cu partenerii, investitorii și alte terțe părți implicate în afacerile companiei.

Așadar, legile privind protecția datelor și confidențialitatea impun gestionarea securității tuturor datelor cu caracter personal deținute de companie (ale personalului sau clienților propriu). În cazul în care aceste date sunt compromise accidental sau deliberat și compania nu implementează măsuri de securitate adecvate, se poate confrunta cu sancțiuni de reglementare.

Riscuri în companie

Este important să vă gestionați riscurile în consecință. După ce are loc un atac, un instrument

eficient de securitate cibernetică sau un plan de răspuns la incident, adică utilizarea unui consultant cibernetic, poate ajuta la:

- reduce impactul atacului
- raportați incidentul autorității competente
- curățați sistemele afectate
- puneți în funcțiune afacerea dvs. în cel mai scurt timp posibil.

Este necesar să se investească în formarea și educarea utilizatorilor în domeniul securității cibernetice pentru a evita atacurile și a dezvolta în mod continuu conștientizarea pentru o strategie cibernetică în organizația proprie.

Cadrul de securitate cibernetică

Un cadru de securitate cibernetică este un set de bune practici și procese documentate care sunt utilizate pentru a dezvolta politici de securitate IT în cadrul unei organizații. Dar, spre deosebire de politica tradițională strict legată de domeniul juridic, un cadru de securitate cibernetică ar trebui să includă, de asemenea, exemple documentate de probleme care trebuie evitate prin acele politici și ale proceselor și modalităților adecvate de implementare a politicilor de securitate descrise în cadru.

Este atât un ghid pentru angajați și utilizatori, cât și un compendiu convingător de bune practici de securitate care poate fi consultat de părți externe autorizate (cum ar fi autoritățile). Un cadru de competențe de securitate cibernetică poate ajuta, de asemenea, la o mai bună evaluare a competențelor necesare pentru a evita atacurile, lacunele și măsurile de remediere.

Securitate cibernetică

În ciuda gradului de conștientizare sporit și a eforturilor îndrăznețe, este cunoscută penuria extrem de semnificativă și tot mai mare de profesioniști în securitate cibernetică în Uniunea Europeană și cunoștințele și abilitățile angajaților pentru a evita atacurile cibernetice la nivel mondial, iar aceste lipsuri continuă să prezinte probleme majore pentru sectorul public și privat. .

Studiul 2019 CYBERSECURITY WORKFORCE 2019 Strategies for Building and Growing Strong Cyber Security Teams (ISC) estimează că există 2,8 milioane de profesioniști în securitate cibernetică la nivel global, în timp ce decalajul este de fapt de 4,07 milioane.

Studiul notează că decalajul actual în Europa este de 291.000, iar acest număr s-a dublat față de anii precedenți. Multe țări cu expertiză foarte dezvoltată preferă să creeze propriul set de reglementări și documente, dar multe țări și companii mici și mijlocii (IMM-uri) au nevoie de ajutor în acest

context.

Inginerie sociala

- înseamnă manipularea ființelor umane, (folosind adesea metode psihologice), pentru a obține acces la date, documente și informații de interes pentru atacator.
- este una dintre principalele amenințări la adresa securității informațiilor în prezent și este o formă eficientă de criminalitate cibernetică.
- ar putea avea repercusiuni periculoase, de exemplu, încălcări ale datelor, mai mult decât orice alt tip de atac.
- atacurile au un scop financiar și astfel organizațiile au pierdut sume considerabile de bani.
- este deosebit de periculos deoarece se bazează mai mult pe eroarea umană decât pe vulnerabilitățile din software și sisteme de operare.

Companiile:

- ar putea suferi pierderi de productivitate, o scădere a moralului angajaților și dificultăți de recuperare.
- au prejudicii reputației deoarece clienții nu sunt convinși că organizația se poate proteja.
- deseori trebuie să declanșeze un răspuns la incident vechi.
- ar trebui să furnizeze software de securitate pentru a ajuta la prevenirea atacurilor viitoare.
- deseori ar trebui să recalifice angajații pentru a fi pregătiți pentru atacuri.

Inginerie sociala; Instruire (conștientizare cibernetică)

- de angajați și manageri pentru care este important să recunoaștem atacurile de inginerie socială deoarece riscul de a deveni victimă este mare.
- ar putea fi incluse în programe de conștientizare a securității comunitare, individuale și cetățenești și să protejeze indivizii și organizația acestora.
- lipsește în special IMM-urile care au mai puține resurse, așa că ar trebui ajutate să ia în serios formarea de conștientizare cibernetică și să ofere angajaților oportunități de a o lua.

Instruire și mentorat

Antreprenorii, inclusiv cei viitori, au nevoie de moduri complexe de gândire și de capacitatea de a înțelege și integra cunoștințe din diferite sectoare, ceea ce necesită o învățare interdisciplinară. Problemele complexe de inginerie necesită crearea unei situații interdisciplinare într-un mod aproape natural.

Într-o abordare interdisciplinară, cursanții ar trebui să integreze informații din diferite discipline și domenii. Ei dezvoltă o înțelegere interdisciplinară, învață să integreze domenii de expertiză și moduri de gândire specifice disciplinei.

Acest lucru crește abilitățile cognitive și gândirea critică mai mult decât prin mijloace disciplinare unice.

Abilități antreprenoriale și mentorat

Evaluarea performanței cursanților în dezvoltarea abilităților antreprenoriale poate avea o viziune holistică, inclusiv o privire asupra mediului de învățare și a rezultatelor învățării și poate facilita învățarea interactivă, eficientă și activă.

Mentoratul este o metodă cu experiență pentru a sprijini mai multă învățare individuală și pentru a dobândi abilități personale și de carieră pentru noi profesii. Există cercetări cu privire la rezultatele mentoratului în general, dar există puține cercetări despre mentorat.

Mentoratul oferă o serie de beneficii pentru angajații care se formează în companii. Mentoratul interdisciplinar în echipă a câștigat importanță în ultimii ani, reflectând nevoia unei schimbări în orientarea mentoratului, pe măsură ce diversele dezvoltări și domenii antreprenoriale sunt din ce în ce mai multidisciplinare.

Mentoratul interdisciplinar și rețelele de mentori pot produce sinergie în grupuri, pot genera idei inovatoare și soluții complexe la provocări și pot crea oportunități de colaborare și muncă.

Concepte, definiții și termeni

Termenul „**ciberspațiu**” a fost inventat în 1982 de William Gibson. Termenul a intrat în viața de zi cu zi în anii 1990 odată cu apariția World Wide Web

infrastructuri cibernetice - infrastructuri de tehnologie a informației și comunicațiilor, formate din sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice;

spațiu cibernetic - mediul virtual, generat de infrastructurile cibernetice, inclusiv conținutul informațional prelucrat, stocat sau transmis, precum și acțiunile desfășurate de utilizatori în acesta;

securitate cibernetică - starea de normalitate rezultată din aplicarea unui set de măsuri proactive și reactive care asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nerepudiarea informațiilor în format electronic, a resurselor și serviciilor publice sau private, în spațiul cibernetic.

Măsurile proactive și reactive pot include politici de securitate, concepte, standarde și linii directoare, managementul riscurilor, activități de formare și conștientizare, implementarea de

soluții tehnice pentru protejarea infrastructurilor cibernetice, managementul identității, managementul consecințelor;

apărare cibernetică - acțiuni desfășurate în spațiul cibernetic în scopul protejării, monitorizării, analizei, detectării, contracarării agresiunilor și asigurării unui răspuns în timp util împotriva amenințărilor la adresa infrastructurii cibernetice specifice apărării naționale;

operațiuni în rețele de calculatoare - procesul complex de planificare, coordonare, sincronizare, armonizare și desfășurare a acțiunilor în spațiul cibernetic de protecție, control și utilizare a rețelelor de calculatoare în vederea obținerii superiorității informaționale, concomitent cu neutralizarea capacităților adversarului;

amenințare cibernetică - circumstanță sau eveniment care constituie un potențial pericol pentru securitatea cibernetică;

atac cibernetic - acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică;

incident cibernetic - eveniment care are loc în spațiul cibernetic, ale cărui consecințe afectează securitatea cibernetică;

terorism cibernetic - activități premeditate desfășurate în spațiul cibernetic de persoane, grupuri sau organizații motivate politic, ideologic sau religios care pot provoca distrugeri materiale sau victime, susceptibile de a provoca panică sau teroare;

spionaj cibernetic - acțiuni desfășurate în spațiul cibernetic, cu scopul de a obține informații confidențiale neautorizate în interesul unei entități statale sau nestatale;

infractiune informatica - totalitatea faptelor prevazute de legea penala sau alte legi speciale care prezinta un pericol social si sunt savarsite cu vinovatie, prin sau pe infrastructuri cibernetice;

vulnerabilitate în spațiul cibernetic - slăbiciune în proiectarea și implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente care pot fi exploatate de o amenințare;

risc de securitate în spațiul cibernetic - probabilitatea ca o amenințare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetice;

managementul riscurilor - un proces complex, continuu și flexibil de identificare, evaluare și contracarare a riscurilor de securitate cibernetică, bazat pe utilizarea unor tehnici și instrumente complexe, pentru prevenirea pierderilor de orice fel;

managementul identității - metode de validare a identității persoanelor atunci când accesează

anumite infrastructuri cibernetice;

Componentele controlului intern

Conform standardului INTOSAI GOV 9100 „Orientări pentru standardele de control intern". În 2001, la Congresul Organizației Internaționale a Instituțiilor Supreme de Audit (INCOSAI), s-a decis actualizarea Ghidurilor INTOSAI pentru standardele de control intern în sectorul public, emise inițial în 1992, prin introducerea în document a tuturor aspectelor evoluțiilor recente. în domeniul controlului intern și să integreze o serie de elemente ale modelului COSO (Internal Control – Integrated Framework).

Prin integrarea acestuia în Ghid - activitate desfășurată de grupul operativ al Comitetului pentru Standarde de Control Intern al INTOSAI - s-a încercat obținerea unei înțelegeri unificate a modului în care funcționează noul sistem de control intern, de către reprezentanții Instituțiilor Supreme de Audit. .

„Liniile directoare ale INTOSAI pentru standardele de control intern în sectorul public" fac parte din categoria INTOSAI GOV (orientări privind buna guvernare) și sunt considerate extrem de utile atât pentru managerii din sectorul public care trebuie să implementeze sistemul de control intern, cât și pentru auditorii publici externi, care trebuie cunoașteți acest sistem și evaluați-l.

Standarde de control intern

Conform Ghidurilor INTOSAI GOV 9100), controlul intern constă din cinci componente interdependente (identice cu cele ale modelului COSO):

- Mediu de control
- Evaluarea riscurilor
- Activități de control
- Informatie si comunicare
- Monitorizarea

Controlul intern este conceput pentru a oferi o asigurare rezonabilă cu privire la realizarea obiectivelor generale ale instituției. Obiectivele clar stabilite de șefii entității și planificarea adecvată a bugetului sunt o condiție obligatorie pentru un control intern eficient.

Mediul de control

Mediul de control cuprinde atitudinea generală, conștientizarea și acțiunile întreprinse de conducere și de cei însărcinați cu guvernanța cu privire la sistemul de control intern și importanța acestuia în cadrul entității. Mediul de control dă tonul organizației, influențând conștiința de

control la nivelul personalului.

Reprezintă baza tuturor celorlalte componente ale controlului intern, asigurând o disciplină în cadrul organizației care trebuie respectată și o structură a entității, astfel încât sistemul de control intern să poată fi aplicat eficient. Mediul de control intern este un instrument eficient în prevenirea corupției și fraudei.

Elementele care definesc mediul de control sunt:

- integritate personală și profesională, valorile etice stabilite de conducere pentru întreg personalul, inclusiv o atitudine permanentă de susținere față de controlul intern;
- o preocupare continuă a managementului pentru competența personalului;
- „tonul dat de sus" (filozofia și stilul de activitate al managementului);
- structura organizatorică a entității;
- Politica și practicile de HR.

Tipuri de controale de securitate cibernetică

Controalele securității cibernetice sunt mecanisme utilizate pentru a preveni, detecta și atenua amenințările și atacurile cibernetice. Mecanismele variază de la controale fizice, cum ar fi agenții de securitate și camerele de supraveghere, până la controale tehnice, inclusiv firewall-uri și autentificare cu mai mulți factori.

O abordare unilaterală a securității cibernetice este pur și simplu depășită și ineficientă. Și pentru că este imposibil să previi toate atacurile în peisajul amenințărilor actuale, organizațiile ar trebui să-și evalueze activele pe baza importanței lor pentru afacere și să stabilească controale în consecință.

La o provocare se adaugă faptul că este puțin probabil ca angajații să respecte regulile de conformitate dacă sunt implementate controale stricte pentru toate activele companiei. Severitatea unui control ar trebui să reflecte direct peisajul activelor și al amenințărilor.

Consecințele expunerii unui hacker de mii de date personale ale clienților printr-o bază de date în cloud, de exemplu, pot fi mult mai mari decât dacă laptopul unui angajat este compromis.

Controale de securitate cibernetică

„Există multe moduri diferite de a aplica controale bazate pe natura a ceea ce încercați să protejați", a spus Joseph MacMillan, autorul cărții Infosec Strategies and Best Practices și cybersecurity global black belt la Microsoft.

„Care este natura amenințării de care încercați să vă protejați?

Este un actor rău intenționat?

Sau este un atac devastator?”

Securizarea activelor informaționale

Se referă la implementarea controalelor adecvate de securitate a informațiilor pentru active. Dorim să ne asigurăm că ne concentrăm pe ideologii puternice și eficiente pentru a înțelege să selectăm controalele adecvate, ceea ce înseamnă că activul este considerat „suficient de sigur” pe baza criticității și clasificării sale. Există diferite clase care împart tipurile de controale:

- Controalele administrative/managementale sunt politicile și procedurile firmei. Nu sunt la fel de „mișto” ca un nou control software, dar există pentru a oferi structură și îndrumare indivizilor și altor membri ai organizației, asigurându-se că nimeni nu este amendat sau nu provoacă o încălcare.
- Controale fizice care limitează accesul la sisteme într-un mod fizic.
- Controalele tehnice/logice sunt cele care limitează accesul pe baza hardware sau software, cum ar fi criptarea, cititoarele de amprente, autentificarea sau modulele de platformă de încredere (TPM).

Ele nu limitează accesul la sistemele fizice, așa cum fac controalele fizice, ci mai degrabă accesul la date sau conținut. Controalele operaționale sunt cele care implică persoane care efectuează procese zilnic. Exemplele ar putea include formarea de conștientizare, clasificarea activelor și examinarea fișierelor jurnal.

Tipuri de controale

Controalele preventive există pentru a preveni o acțiune și includ firewall-uri, garduri și permisiuni de acces.

Comenzile detective sunt declanșate numai în timpul sau după un eveniment, cum ar fi sistemele de supraveghere video sau de detectare a intruziunilor. Elementele de descurajare descurajează amenințările să încerce să exploateze o vulnerabilitate, cum ar fi un semn „Watchdog” sau câini. Controalele corective sunt capabile să ia măsuri de la o stare la alta. Comenzile fail open și fail closed sunt abordate aici.

Comenzile de recuperare primesc ceva înapoi dintr-o pierdere, cum ar fi recuperarea unui hard disk. Controalele de compensare sunt cele care încearcă să compenseze deficiențele altor controale, cum ar fi revizuirea regulată a jurnalelor de acces. Acest exemplu este, de asemenea, un control detectiv, dar controalele de compensare pot fi de diferite tipuri.

Ordinea controalelor

Îi descurajează pe actori să încerce să acceseze ceva ce nu ar trebui să fie. Deny/Prevent Access printr-un control preventiv, cum ar fi permisiunile de acces sau autentificarea.

Detectați riscul asigurându-vă că înregistrați detectarea, cum ar fi cu software-ul de protecție a punctelor terminale. Întârzieți procesul de la repetarea riscului din nou, cum ar fi cu o funcție „prea multe încercări" pentru introducerea unei parole.

Corectați situația răspunzând la compromis, cum ar fi cu un plan de răspuns la incident. Recuperați dintr-o stare compromisă, cum ar fi un generator de rezervă care restabilește disponibilitatea unui server.

În plus, în domeniul îmbunătățirii continue, ar trebui să monitorizăm valoarea fiecărui activ pentru orice modificări. Motivul este că este posibil să fie nevoie să ne regândim controalele pentru protejarea acelor active dacă acestea devin mai mult sau mai puțin valoroase în timp sau în timpul anumitor evenimente majore din organizația dvs.

Controale și recuperare

Când ne uităm la controale, ar trebui să ne gândim și la recuperare, dorim să ne putem recupera din orice situații adverse sau modificări ale activelor și ale valorii acestora. Doar ca exemple, vorbim despre backup-uri, redundanță, procese de restaurare și altele asemenea.

Un concept de reținut, mai ales în era cloud, SaaS, PaaS, IaaS, soluții terță parte și toate celelalte forme de „calculator altcuiva" este acela de a se asigura că Acordurile privind nivelul de servicii (SLA) sunt clar definite și au timp de nefuncționare maxim admisibil. acorduri, precum și penalități pentru nerespectarea acestor acorduri. Acesta este un exemplu de control compensator.

Întrebări:

Forumul de discuții la care se răspunde cu o scurtă explicație. Răspunsurile vor fi discutate cu mentorul în timpul sesiunilor de mentorat

1. Care sunt riscurile din companie pentru atacurile cibernetice?
2. Apelați unele tipuri de controale de securitate cibernetică
3. Vrăjitoare sunt standarde de control intern
4. Cum să controlezi și să recuperezi informații

Întrebări de autoevaluare. După ce răspunde, cursantul poate vedea rezultatele și le poate compara cu cele salvate pe platformă

- Riscuri în companie pentru atacuri cibernetice
- Standarde și reguli de control intern
- Mediu de control

Atasamente

Prezentare PowerPoint

Filme video

Referințe:

- Cyber Attacks on Companies: Are You at Risk?
- The rising strategic risks of cyberattacks
- 10 Common Cyber Security Risks For Businesses
- Internal Controls and Data Security: How to Develop Controls That Meet Your IT Security Needs
- Internal Controls Over Information Systems