Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 6

# La disciplina „Managementul și Auditul Securitații Informaționale”

Tema: “Dosarul auditului intern: plan, program, universul de audit, chestionar.”

A efectuat: st. gr. SI-211 A. Chihai

A verificat: E. Nemerenco

Chișinău – 2024

### 1. Roluri și structuri de securitate

* **Întrebare 1:** "Rolurile și structurile organizaționale dedicate securității sunt bine definite și cunoscute de toți angajații?"
* **Răspuns:** În organizația noastră, rolurile și structurile dedicate securității sunt clar definite în documentația de politici de securitate și sunt comunicate tuturor angajaților prin sesiuni de instruire regulată și materiale accesibile pe intranetul companiei. Fiecare departament are un reprezentant de securitate desemnat care este responsabil pentru implementarea și monitorizarea politicilor de securitate la nivelul departamentului respectiv.
* **Întrebare 2:** "Există un cadru clar pentru revizuirea și actualizarea rolurilor de securitate în funcție de schimbările organizaționale sau tehnologice?"
* **Răspuns:** Aici, auditorul ar trebui să examineze politicile organizației privind revizuirea periodică a rolurilor de securitate și a structurilor organizaționale. Este crucial să se verifice dacă există un mecanism formal pentru adaptarea rolurilor și responsabilităților la noile tehnologii și la restructurările organizaționale. De asemenea, interviurile cu managerii de securitate pot releva cum sunt gestionate aceste schimbări.
* **Întrebare 3:** "Cum sunt gestionate responsabilitățile suplimentare care apar în urma schimbărilor în structura de securitate?"
* **Răspuns:** Se așteaptă ca organizația să aibă procese bine stabilite pentru delegarea și gestionarea responsabilităților noi. Auditorul ar putea investiga protocoalele de comunicare internă, procesele de training pentru noile responsabilități și feedback-ul angajaților despre cum sunt percepute și implementate aceste schimbări.

### 2. Organizarea și pilotarea securității generale

* **Întrebare 1:** "Există un comitet de securitate care să supravegheze toate aspectele legate de securitatea organizațională?"
* **Răspuns:** Un audit eficient ar începe cu identificarea comitetului de securitate și a documentelor care atestă rolul și responsabilitățile acestuia. De asemenea, este important să se verifice frecvența întâlnirilor comitetului și să se revizuiască minutele acestor întâlniri pentru a înțelege cum sunt tratate problemele de securitate.
* **Întrebare 2:** "Cum sunt evaluate și gestionate riscurile de securitate la nivelul întregii organizații?"
* **Răspuns:** Auditorul ar trebui să examineze procesul de evaluare a riscurilor, inclusiv metodele și frecvența acestor evaluări. Este important să se verifice cum sunt prioritizate riscurile și cum sunt implementate măsurile de atenuare. Documentele, cum ar fi rapoartele de evaluare a riscurilor și planurile de acțiune, pot oferi dovezi valoroase.
* **Întrebare 3:** "Ce metode sunt folosite pentru a comunica politici și actualizări de securitate în întreaga organizație?"
* **Răspuns:** O comunicație eficientă este crucială pentru implementarea politicilor de securitate. Auditorul ar trebui să verifice existența unui plan de comunicare și să evalueze canalele folosite (ex. emailuri, bulletin boards, intranet). De asemenea, ar trebui verificată frecvența cu care sunt comunicate actualizările și modul în care sunt primite și înțelese de către angajați.

### 3. Conformitatea cu politicile și standardele de securitate

* **Întrebare 1:** "Cum se asigură organizația că toate politicile de securitate sunt în conformitate cu legile și reglementările relevante?"
* **Răspuns:** Pentru a asigura conformitatea cu legile și reglementările, organizațiile ar trebui să aibă implementat un sistem de management al conformității care include identificarea tuturor cerințelor legale și regulatorii aplicabile. Acest sistem ar trebui să fie susținut de o colaborare strânsă între departamentul de securitate IT și departamentul juridic. Auditorul ar trebui să verifice existența unei documentații care să ateste analiza periodică a legilor și a impactului acestora asupra organizației. De asemenea, ar trebui examinate procedurile de audit intern și extern, pentru a confirma că acestea includ verificarea conformității cu legile relevante.
* **Întrebare 2:** "Ce proceduri sunt în loc pentru a verifica respectarea continuă a standardelor de securitate?"
* **Răspuns:** Procedurile eficiente pentru verificarea respectării standardelor de securitate includ audituri interne regulate, utilizarea software-ului de monitorizare a conformității și sesiuni de training pentru angajați privind importanța respectării standardelor. Auditorul ar trebui să evalueze frecvența și comprehensivitatea auditurilor interne și să verifice cum sunt tratate descoperirile și neconformitățile. Este important de asemenea să se confirme că există un mecanism de feedback prin care angajații pot raporta problemele de conformitate.
* **Întrebare 3:** "Există un proces formalizat pentru revizuirea și actualizarea periodică a politicilor de securitate?"
* **Răspuns:** Un proces formalizat de revizuire și actualizare a politicilor de securitate ar trebui să includă un calendar definit pentru revizuirea periodică a politicilor, proceduri clare de modificare a politicilor și un comitet de securitate sau un responsabil cu gestionarea acestui proces. Auditorul ar trebui să solicite și să revizuiască înregistrările reuniunilor în care se discută politicile de securitate, precum și documentația care atestă implementarea modificărilor. De asemenea, este esențial să se verifice dacă modificările sunt comunicate eficient tuturor părților interesate și dacă există un sistem pentru a colecta feedbackul referitor la implementarea noilor politici.

### 1. Managementul Identității și Accesului (IAM)

* **Întrebare 1:** "Cum sunt implementate și gestionate politicile de minimizare a privilegiilor pentru accesul la resursele AWS?"
* **Răspuns:** Politicile de minimizare a privilegiilor în AWS sunt implementate prin atribuirea de roluri IAM specifice care oferă accesul strict necesar pentru îndeplinirea funcțiilor unui utilizator sau ale unui sistem. Auditul ar trebui să verifice existența unor politici clare pentru definirea și revizuirea rolurilor IAM, utilizarea grupurilor pentru a gestiona permisiuni similare pentru utilizatori multipli și utilizarea AWS Identity and Access Management pentru a aplica aceste politici.
* **Întrebare 2:** "Ce metode sunt folosite pentru a monitoriza și revizui periodic drepturile de acces ale utilizatorilor și ale sistemelor automatizate?"
* **Răspuns:** Metodele includ utilizarea AWS CloudTrail pentru a monitoriza și înregistra toate apelurile API pentru revizuirea accesului la resurse, precum și AWS Config pentru a evalua configurațiile resurselor în raport cu profilurile dorite. Auditul ar trebui să confirme că revizuirile accesului sunt efectuate periodic și că se folosesc tool-uri automate pentru a alerta administrații despre orice modificări neautorizate.
* **Întrebare 3:** "Există mecanisme în loc pentru a asigura autentificarea multifactorială (MFA) pentru accesul la consola AWS și API-uri critice?"
* **Răspuns:** Organizația ar trebui să aibă MFA activat pentru toți utilizatorii care accesează consola AWS și API-uri critice. Auditorul ar trebui să verifice setările de politică IAM pentru a asigura că MFA este obligatorie și să examineze logurile de autentificare pentru a confirma utilizarea efectivă a MFA.

### 2. Securitatea Rețelei

* **Întrebare 1:** "Ce strategii sunt utilizate pentru a securiza grupurile de securitate și setările ACL pentru resursele din VPC?"
* **Răspuns:** Strategiile includ definirea strictă a regulilor de grup de securitate care limitează traficul neautorizat spre și dinspre resursele AWS. ACL-urile (Access Control Lists) sunt setate pentru a oferi un nivel suplimentar de filtrare a traficului. Auditul ar trebui să examineze aceste configurații pentru a asigura că sunt conform cerințelor de securitate și că nu permit accesul excesiv.
* **Întrebare 2:** "Cum sunt implementate zonele demilitarizate (DMZ) și cum sunt segregate rețelele sensibile de restul infrastructurii cloud?"
* **Răspuns:** Zonele DMZ sunt configurate prin VPC-uri separate sau prin subneturi izolate în cadrul unui VPC, cu reguli stricte de grup de securitate și ACL-uri pentru controlul traficului. Segregarea rețelelor sensibile se realizează prin utilizarea VPC peering, subrețele private și gateway-uri NAT pentru a controla traficul între zonele de producție și cele externe. Auditorul ar trebui să verifice aceste aranjamente și să confirme că segregarea este efectivă și conformă cu cele mai bune practici.
* **Întrebare 3:** "Sunt folosite servicii de detectare și prevenire a intruziunilor (IDS/IPS) în cadrul infrastructurii AWS?"
* **Răspuns:** Ideal, organizația utilizează AWS Shield pentru protecția împotriva DDoS și poate integra soluții IDS/IPS terțe sau native AWS pentru a monitoriza și a preveni intruziunile. Auditul ar trebui să verifice implementarea acestor servicii și eficacitatea lor în detectarea amenințărilor.

### 3. Criptarea și Securitatea Datelor

* **Întrebare 1:** "Ce politici și tehnologii sunt utilizate pentru criptarea datelor în repaus și în tranzit?"
* **Răspuns:** Organizațiile ar trebui să utilizeze criptarea datelor atât în repaus cât și în tranzit pentru a proteja confidențialitatea și integritatea datelor. AWS oferă criptare la nivel de server și client folosind diverse algoritmi criptografici. Tehnologiile includ AWS KMS pentru gestionarea cheilor criptografice, SSL/TLS pentru criptarea datelor în tranzit, și EBS encryption pentru datele în repaus. Auditorul ar trebui să verifice politicile de criptare și să confirme că sunt implementate conform celor mai bune practici și cerințelor de conformitate.
* **Întrebare 2:** "Cum sunt gestionate și protejate cheile de criptare, și ce rol joacă AWS Key Management Service (KMS) în acest proces?"
* **Răspuns:** AWS KMS este folosit pentru a crea, gestiona și roti cheile criptografice utilizate pentru criptarea datelor. Cheile sunt protejate în hardware security modules (HSM) care sunt conforme cu standardul FIPS 140-2. Auditorul ar trebui să examineze politicile și procedurile de gestionare a cheilor, inclusiv controlul accesului la chei, rotirea periodică a cheilor și utilizarea cheilor de master și ale cheilor de derivare.
* **Întrebare 3:** "Există proceduri stabilite pentru gestionarea backup-urilor și a datelor arhivate, asigurând confidențialitatea și integritatea acestora?"
* **Răspuns:** Procedurile pentru backup-uri și arhivare ar trebui să includă criptarea datelor, stocarea sigură a backup-urilor și testarea periodică a restaurării datelor pentru a asigura integritatea lor. Auditorul ar trebui să verifice că există un program de backup clar, cu specificații privind frecvența, tipurile de date salvate și securitatea depozitelor de date, împreună cu proceduri testate de restaurare.

### 4. Monitorizare și Logare

* **Întrebare 1:** "Ce sisteme sunt în loc pentru colectarea, stocarea și analiza logurilor de securitate?"
* **Răspuns:** AWS oferă AWS CloudTrail pentru colectarea logurilor activităților API și AWS CloudWatch pentru monitorizarea resurselor și aplicațiilor. Organizațiile ar trebui să configureze aceste servicii pentru a colecta și stoca loguri în mod centralizat, și să folosească soluții de analiză a logurilor pentru a detecta activități suspecte. Auditorul ar trebui să verifice configurarea și utilizarea acestor servicii, precum și politici de retenție și protecție a logurilor.
* **Întrebare 2:** "Cum sunt configurate și monitorizate alertele pentru evenimente de securitate anormale?"
* **Răspuns:** Alertele ar trebui configurate pentru a detecta comportamente și evenimente anormale care ar putea indica tentative de securitate sau falii de sistem. AWS CloudWatch și AWS GuardDuty pot fi folosite pentru a seta alerte pe baza unor threshold-uri predefinite sau anomalii detectate. Auditorul ar trebui să evalueze eficacitatea configurărilor de alertă și să verifice dacă alertele sunt revizuite și actualizate regulat pentru a reflecta schimbările în infrastructură și amenințările emergente.
* **Întrebare 3:** "Sunt implementate soluții de gestionare a evenimentelor de securitate și informații (SIEM) pentru a oferi vizibilitate și răspuns rapid la incidente?"
* **Răspuns:** Soluțiile SIEM, cum ar fi Splunk sau AWS-native services precum Amazon Detective, sunt esențiale pentru analiza datelor de logare și detectarea incidentelor de securitate. Acestea agregă loguri din multiple surse, facilitând detectarea rapidă a incidentelor și coordonarea răspunsurilor. Auditorul ar trebui să verifice integrarea și configurarea soluțiilor SIEM, împreună cu procedurile de răspuns la incidente pentru a asigura o reacție rapidă și eficientă.

**Concluzie:**

Este esențial să se acorde o atenție deosebită fiecărei secțiuni a raportului pentru a înțelege pe deplin modul în care organizația abordează securitatea informațională și pentru a identifica eventualele puncte slabe sau zone de îmbunătățire. Un aspect critic al securității informaționale este adaptabilitatea și capacitatea de a răspunde la amenințări și schimbări în mediul tehnologic și organizațional.

Prin abordarea comprehensivă a diferitelor aspecte ale securității informaționale, organizația poate să-și întărească poziția în fața potențialelor amenințări și să-și protejeze activele și datele sensibile. Este important ca rapoartele de audit să ofere recomandări și sugestii constructive pentru îmbunătățirea continuă a practicilor de securitate și pentru a asigura conformitatea cu standardele și reglementările relevante.

În final, un efort colaborativ între echipele de securitate informațională, conducerea organizației și auditorii poate contribui la consolidarea și îmbunătățirea continuă a securității informaționale în întreaga organizație.