UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI
MINISTERUL MUNCII, FAMILIEI, PROTECŢIEI SOCIALE ŞI PERSOANELOR VÂRSTNICE
AMPOSDRU

Fondul Social European
POSDRU 2007-2013

Instrumente Structurale
2007-2013

MINISTERUL EDUCAŢIEI NAŢIONALE
OIPOSDRU

Universitatea POLITEHNICA din Bucureşti

FONDUL SOCIAL EUROPEAN
Investeşte în oameni!
Programul Operaţional Sectorial pentru Dezvoltarea Resurselor Umane 2007 – 2013
Proiect POSDRU/107/1.5/S/76903 – ***Formarea viitorilor cercetatori-experti prin programe de burse doctorale (EXPERT)***

UNIVERSITATEA **POLITEHNICA** DIN BUCUREŞTI

Facultatea de Automatică şi Calculatoare
Departamentul Ingineria Sistemelor

TEZĂ DE DOCTORAT

Contribuţii privind auditul sistemelor informatice în arhitecturi de tip "Cloud Computing"

Contributions regarding the audit of information systems in "Cloud Computing" architectures

Autor: Ing. Speranţa – Georgiana MATEESCU
Conducător de doctorat: Prof.dr.ing. Valentin SGÂRCIU

Bucureşti 2014

1. INTRODUCERE

1.1 SCOPUL LUCRĂRII

În această lucrare am urmărit tratarea problematicilor existente în arhitecturile de tip cloud computing [1] prin evaluarea lor într-un mod eficient şi relevant. În urma activităţilor de cercetare mi-am propus realizarea unei analize care, pe baza rezultatelor concrete şi materializabile să permită trasarea strategiilor viitoare de IT [2]. Astfel, plecând de la o imagine structurată şi uşor de înţeles asupra arhitecturilor de tip “cloud computing” [3], am analizat circumstanţele în care se poate găsi o companie în raport cu acest model arhitectural. Am conturat astfel trei direcţii de analiză:

- Analiza migrării către arhitecturi de tip cloud [4]
- Analiza arhitecturilor hibride care integrează servicii cloud şi sisteme clasice din interiorul companiei [5]
- Analiza serviciilor cloud [6]

Fiecare dintre aceste direcţii de cercetare oferă foarte multe oportunităţi de dezvoltare şi inovaţie, atât datorită multitudinii de modele arhitecturale existente, clasificate pe tipuri de aplicaţii şi pe industrii specifice, cât şi mulţumită specificului fiecărui flux informaţional care manifestă cerinţe tehnologice specifice.

Scopul lucrării mele constă în oferirea unei abordări eficiente de răspuns la întrebări practice survenite odată cu dezvoltarea tehnologică şi apariţia nevoii de agilitate la nivel IT:

- Când decide o companiei să migreze către arhitecturi de tip cloud?
- Ce se întâmplă cu siguranţa datelor odată ce una din aplicaţii este migrată în cloud?
- Care este gradul de guvernare, gestiune şi operare al cloud-ului?

La toate acestea am oferit soluţii materializate în mecanisme eficiente de evaluare a oportunităţii de migrare, am creat abordări eficiente pentru securizarea datelor, am realizat metodologii de realizare a proceselor de audit şi framework-uri de calcul ai unor factori tehnici şi economici privind arhitecturile cloud.

1.2 ORGANIZAREA PE CAPITOLE A LUCRĂRII

Lucrarea de doctorat este structurată pe opt capitole, fiecare dintre ele prezentând procesele şi conceptele care au condus la construirea unei abordări proprii privind audit în arhitecturile de tip cloud computing.

Capitolul I reprezintă introducerea lucrării de doctorat care are menirea de a oferi o imagine de ansamblu a tezei, prin justificarea alegerii acestei tematici şi prezentarea contextului în care ea a fost elaborată. Plecând de la experienţa mea profesională şi academică, am explicat de ce mi-am concentrat atenţia pe domeniul auditului în cloud computing şi care a fost scopul

acestui studiu de cercetare. În finalul capitolului de introducere am inclus o secţiune destinată terminologie şi conceptelor utilizate pe parcursul redactării lucrării.

Capitolul II reprezintă o prezentare structurată a arhitecturilor de tip cloud computing şi a clasificării lor pe baza mai multor criterii. Capitolul introduce termenul de cloud computing alături de beneficiile si neajunsurile pe care acesta le manifestă, apoi este prezentat modelul de referinţă în astfel de arhitecturi aşa cum este el oferit de CSA. Secţiunea 3 cuprinde modelul de securitate de referinţă pe care l-am utilizat pe parcursul activităţii mele de cercetare. Pe baza modelului de referinţă am prezentat modelele de arhitecturi cloud, clasificate pe criteriul nivelului de servicii folosit şi pe cel al localizării spaţiului de stocare.

Capitolul III prezintă procesul de audit al migrării arhitecturilor tradiţionale către arhitecturi de tip cloud prin punctarea etapelor fundamentale ale acestui proces şi a importanţei pe care acest proces îl are în clasificarea unui proces de migrare ca fiind un succes sau, din contră un eşec.

Capitolul IV prezintă cele două abordări proprii privind protecţia datelor partajate în arhitecturi hibride din perspectiva accesului la date şi transportului, procesării şi stocării datelor.

Capitolul V prezintă procesul de audit al arhitecturilor de tip cloud prin punctarea elementelor fundamentale ale acestui proces şi aspectele pe care el le vizează, definindu-l prin prisma a două componente: factorul de siguranţă şi factorul de rentabilitate

Capitolele VI şi VII reprezintă implementările realizate pentru validarea metodologiei de audit propusă şi descrise în capitolele III şi V. Ele vizează, ambele, aplicaţii din domeniul telecomunicaţiilor.

Concluziile tezei de doctorat sunt structurate pe trei secţiuni şi adresează concluziile generale privind procesele de audit din arhitecturi de tip cloud, contribuţiile personale aduse în domeniul auditului cu accent pe beneficiile pe care le-am obţinut prin depunerea activităţii de cercetare, iar finalul acestui capitol este destinat prezentării dezvoltărilor viitoare pe care îmi propun să le aduc în această arie de cercetare.

2. CLOUD COMPUTING

Cloud computing [10] reprezintă un nou concept arhitectural de gestionare de la distanță al resurselor de procesare și stocare de date. Cloud-ul, ca și concept, își propune eficientizarea utilizării de resurse fizice existente pentru o putere de procesare maximă și o eficacitate sporită semnificativ față de metodele tradiționale de procesare.

Cele mai importante și atrăgătoare caracteristici ale cloud-ului sunt abilitatea de a scala și de a proviziona în mod dinamic puterea de calcul, obținând astfel o optimizare a costurilor beneficiarilor, precum şi abilitatea consumatorilor de a consuma aceste resurse în vederea obținerii unor rezultate maxime, fără a se preocupa de gestionare complexității tehnologiei folosite. Aceste caracteristici au dus la un set de valori obţinute prin implementarea unei arhitecturi cloud:

- Satisfacerea instantanee a necesităților de resurse de calcul;
- Valoare sporită adusă tehnologiilor folosite prin diminuarea costurilor;
- Platforme tehnologice standardizate care facilitează colaborarea;
- Reducerea necesarului de personal specializat pentru suportul tehnologiei.

Odată cu toate aceste avantaje, cloud computing aduce și o serie de riscuri materializate în noua dimensiune dată colaborării între organizații și interacțiunii umane, noile dependințe organizaționale, modele noi de business generate datorită posibilității de satisfacere rapidă a oricăror cerințe de performanță din perspectiva puterii de calcul.

2.1 MODELUL DE REFERINȚĂ AL ARHITECTURILOR DE TIP “CLOUD COMPUTING”

Modelul de referinţă propus de cei de la CSA este bazat pe principii fundamentale din arhitecturi tradiţionale şi pe modelele de referinţă existente [11].

De asemenea acest model este realizat pe baza scenariilor reale de utilizare a cloud computing-ului şi respectă recomandări şi best practice-uri din arhitecturile enterprise, printre care:

- Definirea mecanismelor care asigură încrederea în furnizorul de servicii cloud
- Dezvoltarea de capabilităţi şi tipare pentru mai multe platforme bazate pe standarde open pentru furnizori open-source
- Definirea direcţiilor de securizare a informaţiilor protejate de reglementările juridice
- Facilitarea accesului, administrării şi folosirea datelor în deplină siguranţă
- Arhitectura trebuie să faciliteze identificarea, autentificarea, autorizarea, administrarea şi auditarea serviciilor implementate
- Centralizarea politicilor de securitate, operaţiunilor de mentenanţă şi funcţiilor complementare

- Accesul la informaţii trebuie să fie securizat, dar uşor de obţinut şi rapid
- Trebuie să existe abilitatea de a delega şi de a federa accesul acolo unde specificitatea serviciilor o cere
- Serviciile cloud trebuie să fie uşor de adoptat, consumat şi trebuie să respecte şabloanele de securitate definite de standardele existente
- Arhitectura trebuie să fie elastică, flexibilă şi să aibă caracteristici de multitenancy
- Arhitectura trebuie să adreseze mai multe niveluri de protecţie – de la nivelurile reţea, sistem de operare, până la nivelul aplicaţie.

Figura de mai jos prezintă o imagine de ansamblu a modelului de referinţă oferit de CSA:

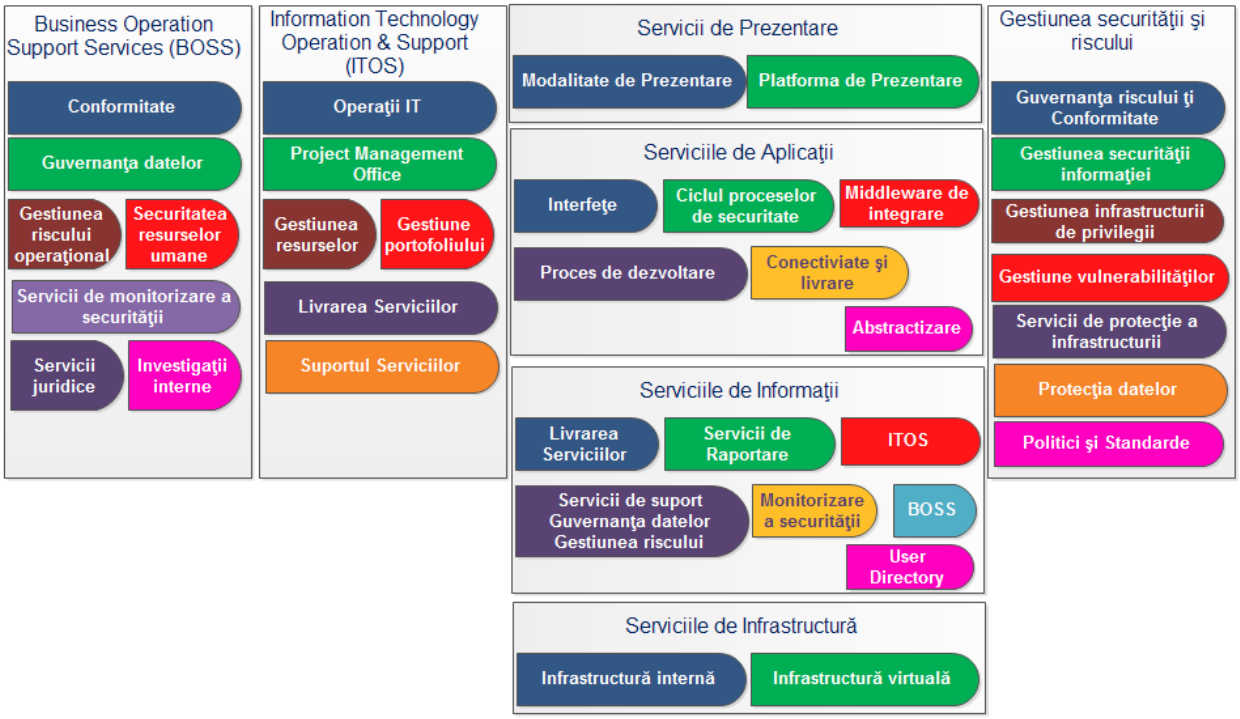

Fig. 2.1: Model de referinţă CSA

Scenariile de bază pe care orice furnizor cloud trebuie să le includă într-o arhitectură cloud sunt:

- Utilizarea aplicaţiilor cloud de către utilizatorii finali
- Utilizarea aplicaţiilor cloud de către companiilor consumatoare de astfel de servicii
- Utilizarea aplicaţiilor cloud de către companii care le pun la dispoziţia utilizatorilor finali

2.2 MODELUL DE SECURITATE AL ARHITECTURILOR DE TIP “CLOUD COMPUTING”

Cloud Security Alliance oferă în [9] un model arhitectural pentru cloud, mapând pe acest model şi cerinţele de conformitate pe fiecare arie arhitecturală. Cloud Security Alliance

categoriseşte aspectele care trebuie avute în vedere în securitatea în următoarele domenii funcţionale:

Tabelul 2.1: Domenii de Securitate în Arhitecturi de tip Cloud

Domeniu	Descriere
Guvernanţa şi gestiunea riscului în medii de tip enterprise	Abilitatea de a guverna şi măsura riscul introdus de cloud computing
Polemici legale: contracte şi vizibilitate asupra mediilor electronice	Legile privind încălcarea măsurilor de securitate informaţională
Gestiunea Conformităţii şi auditului	Evaluarea impactului pe care cloud-ul îl are asupra gradului de conformitate
Gestiunea informaţiilor şi a securităţii datelor	Gestiunea datelor stocate în cloud
Interoperabilitate şi portabilitate	Abilitatea de a migra de la un furnizor de cloud la altul
Mecanisme tradiţionale de securitate, continuitate în business şi recuperarea datelor în caz de dezastru	Impactul pe care îl are cloud-ul asupra procedurilor existente în domeniul securităţii
Operaţiuni la nivel de Data Center	Procedeul de evaluare a Data Center-ului furnizorului de cloud din perspective arhitecturală şi operaţională
Răspunsul în caz de incident	Mecanisme eficiente de detecţie, răspuns la incidente, notificare şi remediere
Securitatea Aplicaţiilor	Securizarea aplicaţiilor care rulează pe diferite modele de arhitectură cloud
Criptarea şi gestiunea cheilor de criptare	Identificarea proceselor eficiente de gestiune şi folosire a cheilor de criptare
Gestiunea identităţilor, rolurilor şi accesului în aplicaţii	Gestiunea identităţilor, rolurilor şi accesului în aplicaţii în modele cloud
Virtualizare	Riscul asociat cu VM isolation, VM co-residence
Security as a Service	Contactarea securităţii ca serviciu de la terţi incluzând şi gestiunea incidentelor şi atestarea conformităţii

Cadrul arhitectural pentru cloud

CSA propune un framework general pentru mediile de tip cloud. IaaS conţine întreaga stivă de resurse de infrastructură – de la funcţionalităţile de bază, până la platformele hardware.

PaaS este situată peste IaaS şi adaugă niveluri de integrare cu framework-uri ce permit dezvoltarea de aplicaţii, capabilităţi middleware şi funcţii ca baze de date, servicii de mesaje şi capabilităţi de prioritizare şi cozi de aşteptare.

SaaS este construit peste cele două modele prezentate mai sus şi conţine medii de gestiune şi procesare a datelor care sunt folosite pentru a livra informaţiile în formatul final către utilizatori – conţinut, prezentare, aplicaţii şi gestiunea capabilităţilor.

Din perspectiva securităţii de date, CSA propune o abordare multi-dimensională a problematicii: implementarea şi consumarea modalităţilor şi serviciilor cloud nu trebuie privită, din perspectivă contextuală, doar ca mediu intern versus mediu extern, ci trebuie

adresată din perspectiva localizării fizice a dispozitivelor, resurselor şi informaţiilor şi a consumatorului de date. În această abordare se impune şi stabilirea celui responsabil de guvernanţa datelor, securităţi şi conformităţii cu politici şi standarde. De asemenea stabilirea şi măsurarea riscurilor introduce la rândul său mai multe dimensiuni:

- Tipul dispozitivelor, resurselor şi informaţiilor gestionate precum şi localizarea lor on sau off premise
- Cine gestionează toate resursele şi cum
- Ce mecanisme de control sunt implementate şi cum sunt acestea integrate
- Problematici privind conformitatea cu legislaţia în vigoare

3. AUDITUL PROCESULUI DE MIGRARE A ARHITECTURILOR TRADIŢIONALE LA ARHITECTURI DE TIP “CLOUD COMPUTING”

Migrarea unei companii către arhitecturi de tip cloud survine datorită avantajelor pe care acestea le oferă [64]. Însă există şi provocări, prima dintre acestea fiind însăşi alegerea tipului de arhitectură ce trebuie folosită: public sau privat.

Între verticalele cele mai importante în alegerea unui tip se arhitectură de cloud se numără:

- *Comparaţie între disponibilitatea şi încărcarea* în fiecare tip de arhitectură – arhitecturile private sunt un mediu controlabil, care oferă medii de calcul similare cu cele din infrastructura publică.
- *Securitate şi conformitate legislativă* [13] – cloud-urile publice sunt uşor de accesat de oricine. Totuşi, ele pot fi victime atacurilor hackerilor. Cloud-urile private oferă un grad de securitate sporit pentru că resursele sunt clasificate din punct de vedere logic.
- *Control şi mentenanţă* [14] – cloud-urile publice oferă utilizatorilor control direct la capacitatea de procesare a resurselor furnizate. Există situaţii în care furnizorii de cloud nu pot modifica infrastructura existentă pentru că afectează toţi clienţii conectaţi (de exemplu aplicarea unui patch sau swap-ul de hardware)

3.1 DEFINIŢIA AUDITULUI PROCESULUI DE MIGRARE CĂTRE ARHITECTURI DE TIP “CLOUD COMPUTING”

Auditul este un proces de evaluare a situaţiei unei companii din perspectiva proceselor de business, a rolurilor angajaţilor în companie şi a mapării acestora pe activităţile zilnice întreprinse, a sistemelor informatice şi a modului în care acestea sunt capabile să asigure confidenţialitate datelor sensibile.

Etapele specifice procesului de audit în migrarea către o arhitectură cloud sunt:

- Etapa premergătoare migrării în cloud
- Etapa de definire a strategiei de migrare în cloud
- Evaluarea furnizorilor
- Implementarea modelului de cloud ales
- Monitorizarea furnizorului
- Monitorizarea companiei din perspectiva securizării datelor

3.2 METODA DE AUDITARE A PROCESULUI DE MIGRARE

Procesul de auditare al migrării în cloud este bazat pe un algoritm de calculare al impactului. *Impactul* reprezintă nivelul de risc asociat procesului de migrare al unei anumite componente, din anumite perspective adresate de întrebarea care impune acel factor de impact.

Fiecare întrebare are multiple răspunsuri posibile, fiecare dintre ele având mai multe scoruri asociate. Scorurile asociate depind de modelul de arhitectură de cloud către care se migrează. Pe durata procesului de audit, auditorul împreună cu expertul trebuie să aleagă un singur răspuns pentru fiecare întrebare.

După finalizarea chestionarului de audit, se realizează următoarele scoruri care reprezintă nivelul de risc pe care îl manifestă ţinta procesului de audit dacă aceasta va fi migrată către modelul pentru care se calculează scorul:

- Scorul aferent modelului de cloud public
- Scorul aferent modelului de cloud hibrid
- Scorul aferent modelului de cloud privat
- Scorul aferent aplicaţiilor dedicate utilizării în interiorul companiei

În procesul de calculare al scorurilor menţionate anterior, se iau în considerare răspunsurile întrebărilor conţinute în chestionarul de audit care adresează următoarele domenii:

- Complexitatea Implementării
- Risc şi Conformitate
- Infrastructură
- Performanţă
- Toate – acest domeniu include întrebări legate de provocări generale pe parcursul procesului de migrare.

În procesul de calculare al scorului unei ţinte a procesului de audit a migrării către arhitecturi cloud, se iau în considerare răspunsurile tuturor întrebărilor cuprinse în chestionarul de audit, dar şi dependinţele între întrebări.

Scorul este calculat folosind următoarea formulă:

$$s_n = \sum_{i=0}^{n} s_{i.}$$, relaţia (3.1)

Unde:

- s_n este scorul aplicaţiei care evaluează răspunsurile a *n* întrebări independente
- s_i este scorul întrebării independente *i*

Dacă există dependinţe între întrebări, scorul este calculat folosind următoarea formulă:

$$s_n = s_{n-1} + s_i \cdot q_{d_i}$$, relaţia (3.2)

Unde:

- s_n este scorul aplicaţiei care evaluează răspunsurile a *n* întrebări

- s_{n-1} este scorul aplicaţiei care evaluează răspunsurile primele *n-1* întrebări independente
- s_i este scorul întrebării *i* care este dependentă de întrebarea q_{d_i}
- q_{d_i} este scorul întrebării de care este dependentă întrebarea curentă.

Pentru evaluarea furnizorilor de servicii cloud se foloseşte scorul general al migrării ca fiind minimul scorurilor individuale calculate. În funcţie de acest scor, se evaluează furnizorii de cloud pentru a se recomanda cel mai potrivit.

Rezultatul final al procesului de audit constă în impactul general asociat ţintei procesului de audit. Acesta este calculat prin medierea impactului rezultat, folosind următoarea formulă:

$$i_{gen} = \frac{s_{gen}}{\Delta_{gen} - \delta_{gen}}, \text{ relaţia (3.3)}$$

Unde:

- i_{gen} este impactul rezultat din procesul de audit
- S_{gen} este scorul general al procesul de audit
- Δ_{gen}este scorul maxim de audit care se obţine prin alegerea răspunsurilor cu cel mai mare impact în urma migrării către modelul care a generat scorul general
- δ_{gen} este scorul minim de audit care se obţine prin alegerea răspunsurilor cu cel mai mic impact în urma migrării către modelul care a generat scorul general

Pentru cuantificarea surplusului de beneficii adus de arhitecturile cloud se calculează factorul de valoare cloud ca fiind:

$$\varphi_{cloud} = 1 - \frac{i_{pbc} + i_{hc} + i_{pc}}{3 \cdot i_{id}}, \text{ relaţia (3.4)}$$

Unde:

- φ_{cloud}este factorul de valoare adus de arhitecturile cloud
- i_{pbc} este impactul rezultat din procesul de audit pentru arhitecturi de cloud publice
- i_{hc} este impactul rezultat din procesul de audit pentru arhitecturi de cloud hibride
- i_{pc} este impactul rezultat din procesul de audit pentru arhitecturi de cloud privat
- i_{id} este impactul rezultat din procesul de audit pentru arhitecturi de interne

Dacă în urma calculării acestui impact se obţine o valoare negativă, înseamnă că arhitectura cloud nu se pretează acelei aplicaţii, ci ea trebuie menţinută în arhitectura tradiţională.

4. INTEGRAREA SISTEMELOR ÎN ARHITECTURI HIBRIDE

Unul dintre cele mai importante aspecte în ceea ce priveşte arhitecturile hibride îl reprezintă partajarea datelor între sisteme într-o manieră sigură, asigurându-se astfel securitatea datelor din perspectiva accesului la date şi protejării datelor în tranzit, în procesare şi în spaţiul de stocare.

În cele ce urmează, am prezentat două abordări eficiente de conectarea a sistemelor din arhitecturi tradiţionale cu sisteme din cloud, integrări ce au obiective diferite:

- Sistemul de Identity Management urmăreşte asigurarea procesului de autentificare, autorizare şi audit al utilizatorilor aplicaţiei cloud
- Mecanism de protecţie a datelor confidenţiale urmăreşte asigurarea procesului de furnizare a datelor cu caracter confidenţial către aplicaţia cloud şi stocare şi manipularea acestora într-o manieră sigură

4.1 GESTIONAREA IDENTITĂŢILOR ÎN ARHITECTURA HIBRIDĂ

Problematica gestiunii de identităţi în arhitecturi hibride

Sistemele dedicate gestiunii identităţilor şi proceselor de autentificare şi autorizare a accesului la aplicaţii şi la datele stocate şi manipulate de acestea operează următoarele noţiuni [15]:

- Identităţi – acest concept este reprezentarea unei persoane care are asociate mai multe atribute şi mai multe conturi în sistemele pe care le foloseşte
- Conturile – acest concept reprezintă un profil asociat într-o aplicaţie care oferă anumite privilegii şi drepturi de acces în sistemul respectiv. Conturile pot fi asociate persoanelor, adică identităţilor dar şi non-persoanelor – acestea fiind conturi administrative necesare operării, administrării, gestionării şi integrării diferitelor sisteme.

Specific unei arhitecturi hibride este faptul că, fiecărui nivel de implementare îi corespund atât conturile sale, cât şi identităţile utilizatorilor – aceştia la rândul lor fiind clasificaţi în funcţie de relaţia lor cu compania consumatoare de servicii cloud.

Sistemul de Identity Management

Sistemul de Identity Management (IdM) folosit în abordarea proprie, operează cu următoarele concepte:

- Sursă autoritară de date – sistem care furnizează datele privind identităţile stocate
- Sistem ţintă – acesta reprezintă orice sistem cu care se integrează soluţia de IdM în care aceasta provizionează utilizatori.

- Rol de aplicaţie – reprezintă cumulul de privilegii şi mecanisme de acces pe care un utilizator le are în aplicaţie.
- Identitate – reprezintă conceptul de modelare al angajaţilor, partenerilor şi colaboratorilor companiei.
- Cont – reprezintă conturile utilizatorilor de IdM provizionate în sistemele ţintă. Acestea pot avea asociate roluri de aplicaţie. Din perspectiva sistemelor ţintă, conturile provizionate de IdM reprezintă utilizatorii de aplicaţii.
- Mecanism de autentificare – reprezintă sursa datelor folosite în mecanismul de autentificare.

Arhitectura soluţiei de Identity Management

Procesul de gestiune a identităţilor în arhitectura hibridă s-a realizat folosind următoarele sisteme:

- Sistemul de Identity Management din interiorul companiei – acest sistem stochează toţi angajaţii companiei şi atributele acestora, împreună cu conturile din aplicaţiile ţintă pe care aceştia le deţin.
- Sistemul de stocare a certificatelor electronice considerat a fi de încredere
- Un sistem în cloud care oferă servicii de raportare - Business Intelligence (BI)

Într-o arhitectură hibridă – care conţine atât sisteme în cloud cât şi sisteme tradiţionale din interiorul companiei, procedura de autentificare include mai mulţi actori:

Identity Provider (IdP) – această componentă eliberează identitatea digitală. În scenariul implementat de mine, IdP este soluţia de Identity Manager din interiorul companiei şi este o sursă de încredere de identităţi pentru serviciul din cloud.

Service Provider (SP) – această componentă oferă acces la servicii identităţilor care au roluri corespunzătoare. În scenariul implementat de mine SP este sistemul de raportare (BI). Această componentă va stoca informaţii cu privire la atributele utilizatorului care au fost folosite în procesările iniţiate de utilizatori, precum şi date referitoare la momentele primirii identităţii cloud şi cel al distrugerii acesteia. Din perspectivă audit, aceste informaţii sunt relevante atât pentru monitorizarea corectitudinii utilizării datelor şi a aplicaţiei, cât şi ca bază de verificare a indicatorilor de performanţă.

Entity – o entitate reprezintă actorul pentru care se fac cererile. În scenariul implementat de mine, entitatea este chiar utilizatorul final.

Identity Verifier – această componentă este sistemul care verifică identitatea digitală. În scenariul implementat de mine, este o abordare puţin diferită, în sensul că, această verificare se face înainte de a se genera identitatea pentru a verifica că entitatea care solicită identitatea

este legitimă. Acest sistem este sistemul de stocare al certificatelor digitale, iar procesul de verificare este iniţiat de Identity Management.

Figura de mai jos prezintă fluxul de informaţii în procesul de generare al unei identităţi:

- Utilizatorul are un token de la furnizorul de servicii cloud care generează parola necesară autentificării la acesta, pe baza unui cod de client furnizat de serviciul cloud.
- Pe computerul aparţinând companiei, pe care utilizatorul îl deţine, există stocat certificatul digital (DC) care conţine, pe lângă informaţiile specifice certificatului (cum ar fi furnizorul, data expirării, identificatorul unic al certificatului etc.), identificatorul unic al angajatului din sistemele companiei şi informaţii referitoare la dispozitivul de unde certificatul este folosit pentru autentificare.

Procesul de autentificare are următorii paşi:

1. Utilizatorul se autentifică la serviciul cloud folosind certificatul digital.

1.1 Serviciul de cloud generează un cod de client pe care îl trimite înapoi utilizatorului.

1.2 Utilizatorul, folosind token-ul primit de la companie, generează parola şi o introduce în fereastra de autentificare a serviciului cloud,

2. Dacă parola generată în pasul 1.2 este corectă, serviciul cloud trimite DC către sistemul de Identity Management împreună cu codul generat la pasul 1.1.
3. Sistemul de Identity Management trimite DC către Depozitul de certificate de încredere pentru a verifica validitatea, legitimitatea şi integritatea datelor acestuia. Toate datele stocate în certificatul digital sunt criptate. De asemenea, pentru comunicaţia între sistemul de Identity Management şi cel de certificate este criptată, folosind o abordare hibridă.
4. Folosind identificatorul unic al utilizatorului din sistemele companiei, IdM generează identitatea digitală pe baza funcţiei utilizatorului.
5. Sistemul de Identity Management criptează identitatea digitală folosind cheia primită de la furnizorul de cloud şi o trimite serviciului.
6. În funcţie de privilegiile pe care le are utilizatorul în aplicaţia cloud, serviciile disponibile îi sunt afişate utilizatorului.
7. După ce se efectuează toate operaţiunile dorite în aplicaţia cloud, identitatea digitală este distrusă de furnizorul de cloud.

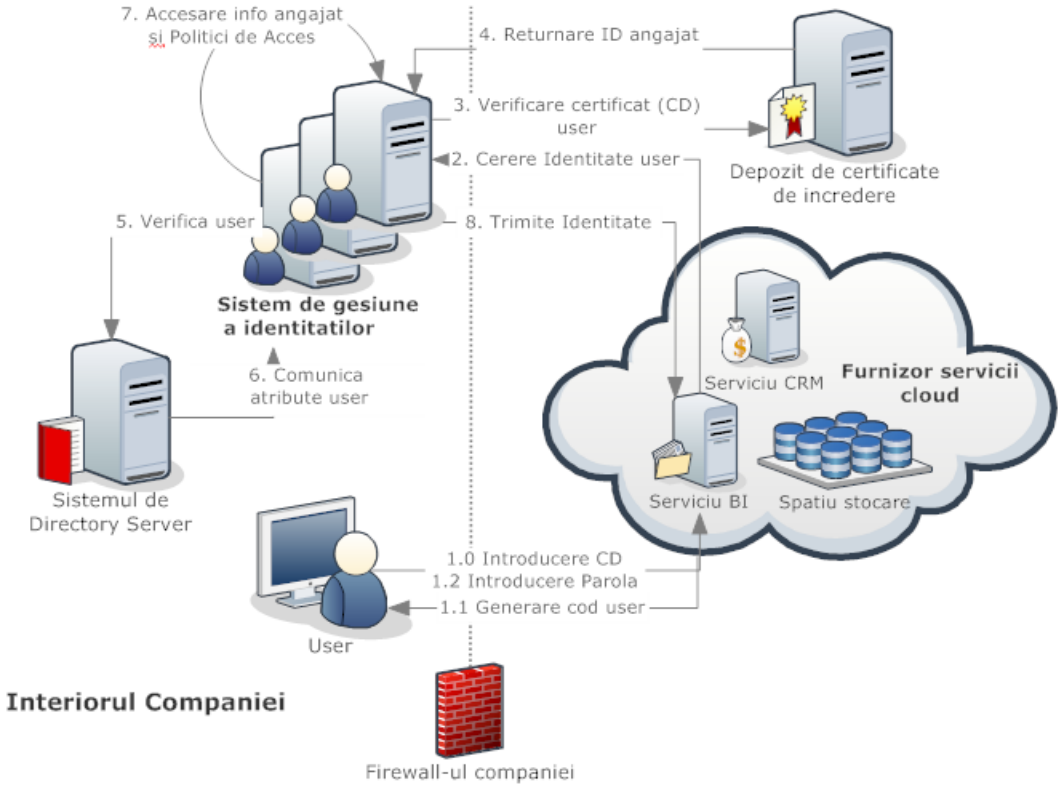

Fig. 4.1: Fluxul de date în generarea unei identităţi digitale

Dacă oricare dintre validările şi verificările descrise mai sus nu este realizată cu succes, un mesaj de eroare este afişat utilizatorului şi accesul la aplicaţia cloud este restricţionat.

Identitatea digitală creată de sistemul de Identity Management conţine următoarele informaţii:

- Informaţii personale despre entitatea care a iniţiat cererea, informaţii necesare pentru a realiza operaţiile dorite care îi sunt permise.
- Date despre drepturile de a accesa informaţiile personale care specifică ce operaţii implementate în aplicaţii cloud pot folosi informaţiile personale.
- Politicile de acces necesare pentru a defini serviciile din aplicaţia cloud la care are acces utilizatorul care a iniţiat cererea
- Informaţii despre sistemul de Identity Management (IdP) – aceste informaţii sunt utilizate pentru a preveni atacul de tipul man in the middle.

Procedeul de utilizare al datelor din identitatea digitală are următoarele etape:

- Serviciul cloud decriptează informaţiile incluse în identitatea digitală
- Serviciul cloud citeşte politicile de acces pentru a-i furniza utilizatorului doar serviciile la care acesta are drept.
- Când utilizatorul realizează o anumită operaţie, aplicaţia cloud accesează informaţiile personale în conformitate cu drepturile de acces incluse în identitatea digitală.

Mecanismul de criptare al datelor transmise între sistemul de IdM şi sistemul de gestiune a certificatelor se bazează pe o abordare hibridă între mecanisme de criptare simetrice şi asimetrice.

Figura de mai jos prezintă mecanismul de criptare:

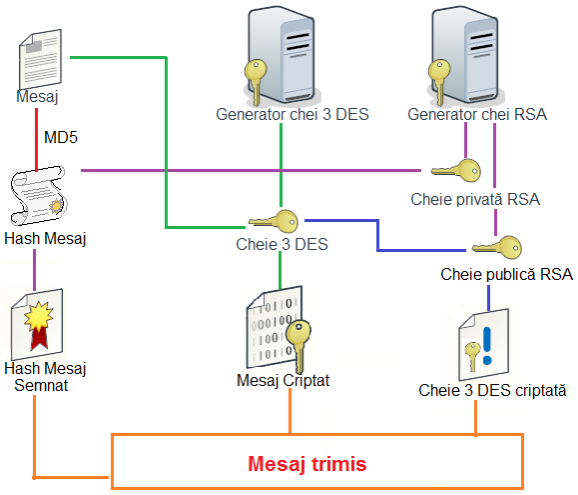

Fig. 4.2: Mecanismul de criptare hibridă

Există două sisteme de generare şi gestionare de chei de criptare:

- Sistemul de generare şi gestionare pentru cheile 3 DES
- Sistemul de generare şi gestionare pentru cheile RSA folosit dedicat pentru comunicaţia dintre sistemul de IdM şi sistemul de gestiune a certificatelor digitale. Acest sistem generează atât cheia publica cât şi cheile private ale sistemelor.

Figura de mai jos prezintă mecanismul de decriptare:

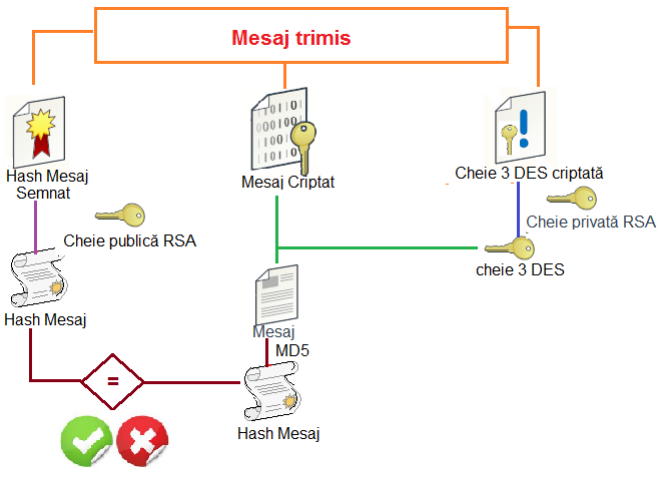

Fig. 4.3: Mecanism de decriptare

Mecanismul de decriptare conţine următorii paşi:

1. Folosind cheia privată RSA, sistemul de gestiune de certificate decriptează cheia 3 DES
2. Folosind cheia 3 DES, se decriptează mesajul. Pentru a se verfica integritatea mesajului, se aplică asupra acestuia algoritmul MD5

3. Folosind cheia publică se verifică hash-ul semnat şi se obţine hash-ul mesajului care se compară cu rezultatul de la pasul 2. Dacă această verificare se realizează cu succes înseamnă că mesajul este integru. Dacă această verificare eşuează, sistemul de gestiune a certificatelor returnează eroare sistemului de Identity Management, aşa încât procesul de generare de identităţi eşuează.

Principalele beneficii ale acestei abordări sunt:

- Utilizatorul nu trebuie să ştie niciodată identitatea sa digitală, fapt ce nu îi permite alterarea drepturilor de acces la aplicaţia cloud
- Există un proces cu 2 paşi de verificare contra furtului de certificate digitale
- Procesul de autentificare implică mai multe sisteme, fapt ce face imposibil un atac de tipul man in the middle cu un singur pas de penetrare.
- Identitatea digitală conţine doar informaţiile necesare serviciilor din aplicaţia cloud care îi sunt permise utilizatorului
- Identitatea digitală este distrusă după ce este folosită, fără a fi stocată în aplicaţia cloud.
- Comunicaţia între sistemele care asigură generarea identităţii digitale este criptată, fapt ce împiedică pierderea datelor confidenţiale în caz de penetrare.

4.2 GESTIONAREA COMUNICAŢIEI DATELOR CONFIDENŢIALE ÎNTRE SISTEMELE DIN INTERIORUL COMPANIEI ŞI CELE DIN EXTERIOR

Criptare 3 DES

DES (Data Encryption Standard) reprezintă un mecanism de criptare simetrică bazat pe chei constituite din blocuri numerice, care a fost realizat de NIST. Astfel, algoritmul are drept intrare un bloc text de 64 de biţi, iar la ieşire un text criptat de aceeaşi dimensiune prelucrat folosind o cheie de 56 de biţi. Procesul de criptare se realizează în trei paşi:

- Permutarea iniţială
- Iterarea mesajului folosind funcţia Feistel
- Aplicarea permutării iniţiale inversă

Criptarea Homomorfică

Criptarea homomorfică reprezintă procesarea datelor criptate astfel încât prin decriptarea rezultatului final să se obţină datele iniţiale procesate. Criptarea homomorfică se bazează pe latici (mulțime ordonată care are proprietatea că orice parte finită a sa are un majorant și un minorant).

Principalele caracteristici ale acestei metodologii de criptare sunt:

- Securizarea datelor şi a funcţiilor de procesare, fapt ce o face deosebit de utilă şi avantajoasă pentru aplicaţiile care presupun procesări ale mai multor sisteme şi delegări computaţionale
- Maleabilitate ţintă – această proprietate presupune că numai un set de funcţii specifice pot modifica datele criptate pentru păstrarea consistenţei lor.
- Putere de calcul şi posibilităţi de verificare – aceste două caracteristici se referă la posibilităţile pe care le proprietarul datelor de a verifica sistemul care a realizat procesarea în vederea stabilirii corectitudinii acesteia.
- Gradul de potrivire între datele criptate şi datele criptate procesate
- Calcul paralel – pentru funcţiile de procesare care permit calculul paralel, acesta poate fi folosit şi pentru criptarea homomorfică, sporind astfel performanţele.

Abordare proprie privind securizarea datelor în arhitecturi hibride

Cea de-a doua preocupare în ceea ce priveşte protejarea datelor cu caracter sensibil partajate de sisteme, în arhitecturi hibride vizează securizarea datelor în tranzit, în procesare şi a datelor stocate

Arhitectura mediului folosit pentru implementarea acestui mecanism de securitate este definită de următoarele particularităţi:

- Aplicaţia de retenţii se află în interiorul companiei şi stochează date confidenţiale despre informaţiile financiare ale clienţilor companiei. Datele stocate sunt criptate folosind un algoritm simetric 3 DES.
- Pentru implementarea algoritmului de criptare se foloseşte un sistem dedicat de gestiune şi generare a cheilor de criptare
- Aplicaţia de raportare cloud comunică cu aplicaţia de retenţii prin web service securizat printr-un mecanism de autentificare
- Aplicaţia de retenţii oferă datele solicitate serviciului cloud criptate, folosindu-se un algoritm homorfic [16] ale cărui chei de criptare sunt generate şi gestionate de un sistem dedicat.

Flux informaţional se realizează conform figurii de mai jos:

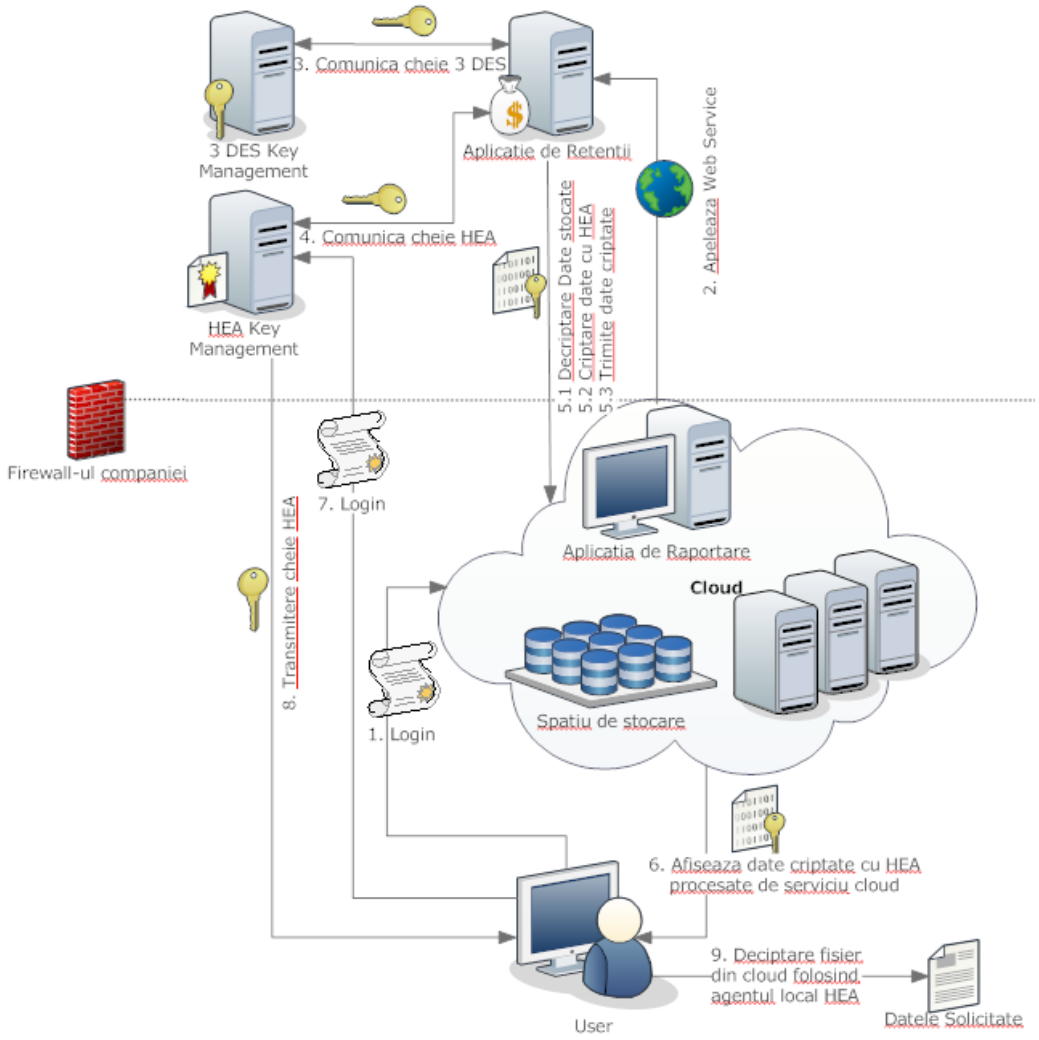

Fig. 4.4: Procesul de securizare a comunicaţiei în arhitecturi hibride

Integrarea între cele două aplicaţii se realizează astfel:

1. Utilizatorul se autentifică la aplicaţia de raportare prin introducerea credenţialelor.
2. Aplicaţia de raportare se conectează la aplicaţia de retenţii prin invocarea unui web service cu mecanism de autentificare şi solicită datele de care are nevoie în vederea rezolvării solicitării utilizatorului
3. Aplicaţia de retenţii comunică cu sistemul intern de gestiune a cheilor de criptare pentru algoritmul 3 DES şi, folosind cheia de decriptare pe care acesta i-o trimite, decriptează datele solicitate de aplicaţia de raportare
4. Aplicaţia de retenţii comunică cu sistemul intern de gestiune a cheilor de criptare pentru algoritmul HEA (Homomorphic Encryption Algorithm)
5. Folosind cheia de criptare pe care sistemul intern de gestiune a cheilor de criptare pentru algoritmul HEA i-o trimite, aplicaţia de retenţii criptează datele solicitate de aplicaţia de raportare şi i le trimite acesteia

6. Aplicaţia de raportare procesează datele criptate şi le trimite utilizatorului ca răspuns la solicitarea sa
7. Agentul instalat pe staţia de lucru a utilizatorului se autentifică cu reţeaua internă a companiei
8. Odată autentificat, agentul obţine cheia de decriptare pentru algoritmul HEA folosit la pasul 5 de aplicaţia de retenţii
9. Agentul instalat la nivelul browser-ului staţiei de lucru decriptează informaţia primită de la aplicaţia de raportare implementată în cloud.

Principalele avantaje ale acestei abordări sunt:

- Toate datele confidenţiale sunt stocate criptat, chiar şi cele din interiorul companiei, fapt ce asigură atât conformitatea cu standardele şi reglementările în vigoare cât şi un grad sporit de protecţie împotriva atacurilor informatice
- Există trei mecanisme folosite pentru asigurarea AAA:
    - Mecanismul de autentificare al aplicaţiei cloud la aplicaţia de retenţii
    - Două mecanisme de autentificare a utilizatorului final
- Chiar dacă există un eveniment de atac soldat cu accesul neautorizat la datele stocate în aplicaţia migrate în cloud, atacatorul nu va putea dispune de aceste informaţii

5. AUDITUL ARHITECTURILOR DE TIP “CLOUD COMPUTING”

5.1 DEFINIŢIA PROCESULUI DE AUDIT AL ARHITECTURILOR DE TIP “CLOUD COMPUTING”

Procesul de audit al arhitecturilor de tip cloud computing reprezintă practica prin care se asigură respectarea anumitor standarde, metode şi practici aplicabile acestui tip de arhitectură.

Arhitecturile de cloud implementează modele de securitate specifice, care, plecând de la conceptele din arhitecturile tradiţionale [17], se materializează în mecanisme specifice. Aceste modele, din perspectiva securităţii includ:

- Securizarea la nivel de arhitectură
- Securizarea la nivel de date
- Securizarea la nivel strategic prin implementarea *best practice*-urilor existente
- Evaluarea securităţii

De aceea, se observă în cadrul arhitecturilor de tip cloud computing o tendinţă de adoptare a framework-urilor de control folosite în sistemele tradiţionale [18]. Cei mai mulţi dintre auditori consideră că infrastructura cloud este asemănătoare cu cea tradiţională, însă există anumite domenii pe care trebuie să se pună accent în arhitecturile cloud şi care trebuie îmbunătăţite faţă de arhitecturile tradiţionale. Există domenii de audit care pot introduce riscuri suplimentare şi care trebuie analizate suplimentar în arhitecturi de tip cloud. Acestea includ:

- Latenţă în comunicarea dintre reţeaua internă a companiei şi cea a furnizorului.
- Notificări în caz de acces neautorizat la datele stocate la furnizorul de cloud.
- Legi internaţionale privind stocare, accesarea şi procesarea datelor confidenţiale.

Procesul de audit în cloud trebuie să se supună aceloraşi principii de audit ca şi procesul de audit din infrastructuri standard [80], printre care se numără: imparţialitatea şi obiectivitatea echipei de audit în analizarea conformităţii arhitecturii cloud, independenţa echipei de audit, principiile practice profesionale de audit, competenţa tehnică de auditare, redactare conformă a rapoartelor de audit.

5.2 FRAMEWORK-URI DE CONTROL PENTRU ARHITECTURI DE TIP CLOUD

COBIT

COBIT 5 reprezintă un framework implementat de ISACA [7] pentru standardizarea măsurilor de guvernanţă şi gestiune a componentelor IT din cadrul unei organizaţii. COBIT adresează controale dezvoltate pentru evaluarea riscurilor din domeniul IT. Aceste controale sunt clasificate în următoarele domenii:

- Planificare şi Organizare (PO) – asigură direcţiile de dezvoltare care trebuie urmate de soluţia livrată şi de serviciul livrat
- Achiziţie şi Implementare (AI) – oferă soluţii care apoi se transformă în servicii
- Livrare şi Suport (DS[1]) – primeşte ca şi intrare soluţiile şi le face utile utilizatorilor
- Monitorizare şi Evaluare (ME) – monitorizează toate procesele pentru a se asigura că acestea urmează calea dorită

COBIT oferă şapte criterii ce trebuie analizate în raport cu informaţiile existente în procesul de guvernanţă şi gestiune:

- Eficacitate[2]
- Eficienţă[3]
- Confidenţialitate[4]
- Integritate[5]
- Disponibilitate[6]
- Conformitate[7]
- Fiabilitate[8]

ISACA a realizat un model de procesare a tuturor capabilităţilor unei companii din perspectiva guvernanţă şi gestiune de componente IT.

Figura de mai jos prezintă modelul procesului de evaluare a capabilităţilor proceselor IT:

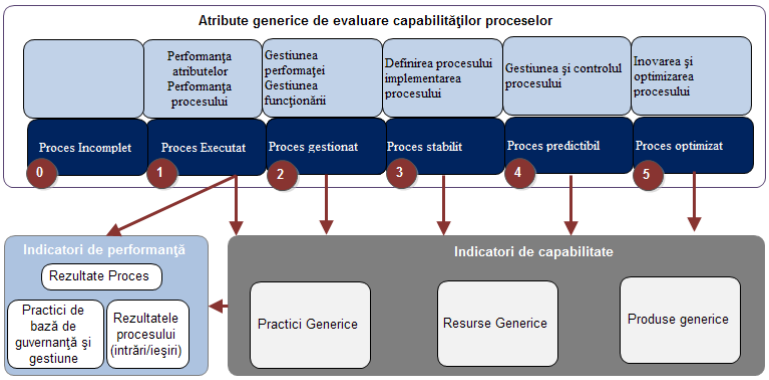

Fig. 5.1: Modelul procesului de evaluare a capabilităţilor proceselor IT [7]

[1] Delivery and Support
[2] O companie este eficace dacă informaţiile sunt relevante şi pertinente procesului de business şi sunt livrate în timp util, asigurând consistenţa şi corectitudinea datelor
[3] O companie este eficientă dacă informaţiile sunt provizionate folosind gradul de utilizare optim al resurselor – cel mai productiv şi economic
[4] O companie asigură confidenţialitatea datelor dacă informaţiile sensibile sunt protejate împotriva folosirii neautorizate
[5] O companie asigură integritatea datelor informaţiile sensibile sunt protejate împotriva folosirii neautorizate
[6] Disponibilitatea este asigurată dacă informaţiile pot fi obţinute când nevoie de ele în procesele de business şi sunt stocate întotdeauna sigur
[7] Compania este capabilă să adreseze procese care dovedesc respectarea standardelor, legilor, reglemetărilor juridice şi clauzelor contractuale aplicabile proceselor de business
[8] Sistemele IT oferă procese de gestiune cu informaţii relevante care sunt utilizate în domeniul operaţional

Există şase niveluri de capabilitate pe care un proces le poate avea, incluzând stadiul de "proces incomplet" dacă operarea lui nu generează scopul acelui proces:

0. Proces Incomplet[9]
1. Proces executat[10]
2. Proces gestionat[11]
3. Proces stabilit[12]
4. Proces predictibil[13]
5. Proces optimizat[14]

Fiecare nivel de capabilitate poate fi obţinut numai când nivelul înaintea lui a fost atins cu succes.

Programul de auditare şi gestionare a arhitecturilor de tip cloud computing

ISACA a realizat, de asemenea "Programul de auditare şi gestionare a arhitecturilor de tip cloud computing" [19] care descrie o metodă de analizare a mecanismelor de control oferite de furnizorii de cloud.

Acest instrument de analiză şi evaluare este realizat pe baza COBIT [7] şi COSO (Committee of Sponsoring Organizations of the Treadway Commission). Aceste componente au drept obiective:

- Stabilirea unor mecanisme de evaluare a controalelor interne folosite de către furnizorii de cloud pe care părţile interesate le pot folosi în procesul de audit
- Identificarea deficienţelor în procesul de control realizat de consumatorul de cloud furnizorului de servicii
- Stabilirea unor mecanisme de evaluare a calităţii serviciilor contractate de la furnizorul de cloud şi de atestare a mecanismelor de control intern implementate de furnizor în arhitectura cloud

Modelul Val IT pentru arhitecturi de tip Cloud

Acest model este folosit în companiile care migrează către cloud pentru evaluarea valorii aduse de implementarea arhitecturilor de tip cloud. Folosind o abordare structurată pe patru

[9] La acest nivel se află procesele care nu sunt implementate sau procesele a căror implementare nu ating obiectivele pentru care procesul a fost creat. La acest nivel există foarte puţine realizări sistematice în ceea ce priveşte scopul procesului

[10] Procesul a fost executat şi şi-a atins obiectivele pentru care a fost creat

[11] Procesul executat la nivelul anterior este implementat folosind o abordare care permite gesionarea lui, iar rezultatele lui pot fi stabilite, controlate şi întreţinute.

[12] Procesul descris la nivelul anterior este implementat folosind un proces definit capabil să obţine rezultate.

[13] Procesul descris la nivelul anterior este operat în limitele definite pe parcursul proiectării procesului în vederea obţinerii rezultatelor scontate

[14] Procesul descris la nivelul anterior îmbunătăţit în mod continuu pentru a se obţine obiectivele relevante pentru care el a fost construit şi definit.

arii diferite, Val IT oferă o perspectivă holistică de cuantificare a valorii adusă de implementarea serviciilor cloud în arhitecturi tradiţionale.

5.3 METODE DE AUDITARE A ARHITECTURILOR DE TIP "CLOUD COMPUTING"

Evaluarea factorului de Siguranţă

Procesul de audit este realizat sub forma unor chestionare ce adresează mecanismele de securitate care asigură un grad sporit de siguranţă, clasificate pe diferite domenii. Fiecare mecanism de securitate are şase niveluri de implementare, auditorul trebuind să selecteze pe cel aplicabil serviciului cloud analizat. Aceste niveluri sunt descrise în tabelul de mai jos.

Tabelul 5.1: Niveluri de implementare a mecanismelor de siguranţă de către furnizorii de cloud

Nivel	Nume Nivel
0	Non-existent
1	Initial
2	Repeatable
3	Defined
4	Managed
5	Optimised

Factorul de siguranţă calculat de aplicaţia de audit este dependent de următoarele mărimi:

- Riscul aplicaţiei supusă analizei din perspectiva domeniului evaluat.
- Gradul de sensibilitate al aplicaţiei
- Riscul asumat al aplicaţiei supusă analizei din perspectiva domeniului evaluat.

Riscul aplicaţiei reprezintă factorul de incertitudine pe care îl manifestă securitatea aplicaţiei cloud în raport cu vulnerabilităţile existente în domeniul adresat de procesul de evaluare al riscului. Altfel spus, riscul aplicaţiei este calculat pe fiecare domeniu în parte.

Valoarea riscului aplicaţiei din perspectiva domeniului analizat este dată de expresia:

$$RA_i = c_{NSA} + \sum_{k=1}^{n}(5 - s_k) \cdot c_A, \text{ relaţia (5.1)}$$

Unde:

- RA_i este riscul aplicaţiei în raport cu domeniul i
- c_{NSA} este constanta de corecţie a riscului[15]
- s_k este gradul de implementare al mecanismului de securitate k
- c_A este constanta de corecţie aplicată riscului aferent unui mecanism de securitate[16]
- n este numărul total de mecanisme de securitate incluse în chestionarul de audit

Riscul asumat al aplicaţiei din perspectiva domeniului evaluat este influenţat de nivelul de risc asumat specificat în definiţia aplicaţiei cloud. Riscul asumat al aplicaţiei este:

[15] Este egală cu valorea minimă a constatelor de corecţie introduse în calcularea riscului. Ea are valoarea de 0.01 şi este introdusă din considerente practice: nu există niciun domeniu care are risc asociat 0.

[16] Constanta de corecţie aplicată riscului este stabilită înainte de procesul de audit în funcţie de industria în care activează compania supusă analizei şi de domeniul şi datele manipulate de aplicaţia evaluată.

$$AR_i = N_r \cdot n \cdot c_A, \text{ relaţia (5.2)}$$

Unde:

- AR_i este riscul asumat pentru aplicaţia analizată în raport cu domeniul *i*
- N_r este nivelul de risc asumat al aplicaţiei
- *n* este numărul total de mecanisme de control din domeniul *i*

Factorul de siguranţă al aplicaţiei supusă analizei în raport cu domeniului evaluat este:

$$FS_i = \frac{5n(1-c_A) - {RA_i}/{AR_i}}{5n} \cdot 100, \text{ relaţia (5.3)}$$

Unde:

- FS_i este factorul de siguranţă al aplicaţiei în raport cu domeniul *i*
- RA_i este riscul aplicaţiei în raport cu domeniul *i*
- AR_i este riscul asumat pentru aplicaţia analizată pentru domeniul *i*
- c_A este constanta de corecţie aplicată riscului aferent unui mecanism de securitate
- *n* este numărul total de mecanisme de securitate

Factorul de siguranţă este exprimat procentual în raport cu gradul ideal de siguranţă care este considerat a fi obţinut în ipoteza în care nu există risc asociat acelui domeniu. Pentru calcularea factorului total de siguranţă, aplicaţia de audit foloseşte următoarea relaţie:

$$FS = \begin{cases} FS_i, \text{ dacă } auditul\ adresează\ un\ domeniu \\ \frac{\sum_{i=1}^{n} FS_i}{n}, \text{dacă } auditul\ adresează\ n\ domenii \end{cases}, \text{ relaţia (5.4)}$$

Unde:

- *FS* este factorul total de siguranţă
- FS_i este factorul de siguranţă al aplicaţiei în raport cu domeniul *i*
- *n* este numărul de domenii evaluate în procesul de audit

Pentru stabilirea gradului de conformitate cu criteriile analizate, s-a calculat factorul minim de siguranţă ca fiind definit de:

$$FS_{min} = 1 - N_r \cdot c_c, \text{ relaţia (5.5)}$$

Unde:

- FS_{min} este factorul minim de siguranţă în raport cu care se evaluează conformitatea
- N_r este nivelul de risc asumat.
- c_c este constanta de conformitate şi este:

Tabelul 5.2: Constanta de conformitate în funcţie de nivelul de risc asumat

Nivel de Risc = N_r	Constantă de conformitate = c_c
1	0.001
2	0.25
3	0.33

Gradul de conformitate al unui domeniu în raport cu standardele este definit de relaţia:

$$NC_i = \frac{1-(-1)^c}{2}\left(FS_{min} + \frac{FS_i - FS_{min}}{FS_{min}}\right)$$, relaţia (5.6)

Unde:

- NC_i este nivelul de conformitate al domeniului i
- FS_{min} este factorul minim de siguranţă în raport cu care se evaluează conformitatea
- FS_i este factorul de siguranţă al domeniului i
- c este conformitatea domeniului i[17]

Evaluarea factorului de rentabilitate al arhitecturilor cloud

Evaluarea factorului de rentabilitate este implementată sub forma unor chestionare ce adresează metrici de procese care trebuie analizate în stabilirea valorii adăugate adusă de programul/portofoliul respectiv, metrice ce sunt clasificate pe diferite domenii. Fiecare metrică are şase niveluri de maturitate. Procesul de audit este bazat framework-ul oferit de Val IT [16]. Pentru fiecare metrică de proces sunt definite niveluri de implementare din care auditorul trebuie să selecteze cel mai potrivit răspuns.

Tabelul 5.3: Niveluri de implementare a mecanismelor de siguranţă de către furnizorii de cloud

Nivel	Nume Nivel
0	Non-existent
1	Initial
2	Repeatable
3	Defined
4	Managed
5	Optimised

Factorul de rentabilitate calculat de aplicaţia de audit este dependent de următoarele mărimi:

- Nivelul aşteptat de maturitate al programului auditat
- Investiţiile totale realizate în programul din care face parte aplicaţia supusă analizei.
- Costul investiţiilor realizate în programul auditat şi durata programului
- Venitul mediu estimat pentru programul din care face parte aplicaţia supusă analizei.
- Costul operaţional aşteptat pentru programul auditat şi riscul asociat aplicaţiei

Factorul de rentabilitate al investiţiei reprezintă rata de fructificare a surselor de finanţare imobilizate sub forma investiţiei. Factorul de rentabilitate este dat de valoarea actualizată netă a programului care este direct impactată de gradul de maturitate al metricilor proceselor.

Scorul de maturitate reprezintă gradul de maturitate al proceselor care implementează programului supus analizei şi este dat de expresia:

$$SM = \frac{\sum_{i=1}^{m} sm_i}{m}$$, relaţia (5.7)

Unde:

[17] Valoarea cestei constante este 0 dacă $FS_{min} > FS_i$ şi 1 altfel

- *SM* este scorul de maturitate al programului supus analizei
- sm_i este scorul de maturitate al metricii *i*
- *m* este numărul total de metrici de proces incluse în chestionarul de audit

Pe baza scorului de maturitate, se calculează indicele de nerealizare:

$$i_n = \frac{1+(-1)^r}{2}(1 - i_r), \text{ relaţia (5.8)}$$

Unde:

- i_n este indicele de nerealizare al programului supus analizei
- i_r este indicele de realizare al programului supus analizei[18]
- r este realizarea programului/portofoliului supus analizei[19]

Indicele de nerealizare are impact direct în rata de actualizare.

Rata de actualizare este metoda prin care se asigură comparabilitatea parametrilor economici şi a indicatorilor financiari ce se realizează în perioade diferite de timp. Pentru exprimarea factorului de rentabilitate a unei aplicaţii din arhitecturi cloud, rata de actualizare este:

$$i = i_n + c_i + R, \text{ relaţia (5.9)}$$

Unde:

- *i* este rata de actualizare folosită pentru calculul factorului de rentabilitate
- i_n este indicele de nerealizare al programului supus analizei
- c_i este costul investiţiei asociată programului din care face parte aplicaţia analizată
- *R* este factorul de risc asociat cu aplicaţia analizată

Factorul de risc este calculat ca fiind media riscurilor asociate cu domeniile supuse procesului de audit care are drept obiectiv evaluarea siguranţei unui serviciu cloud, mediată de numărul total de domenii, astfel:

$$R = \frac{\sum_{k=1}^{n} 1-FS_k}{n}, \text{ relaţia (5.10)}$$

Unde:

- *R* este factorul de risc asociat cu aplicaţia analizată
- *n* este numărul total de domenii supuse procesului de audit
- FS_k este factorul de siguranţă aplicaţiei în raport cu domeniul *k*

Valoarea actualizată netă (VAN) reprezintă o metodă de evaluare a investiţiilor care este direct dependentă de costurile implicate şi de veniturile pe care acestea le generează. Formula de calcul a acesteia este:

[18] Este raportul între scorul de maturitate calculat şi cel aşteptat

[19] Este 1 dacă $i_r \geq 1$, 0 altfel

$$VAN = \sum_{j=1}^{y} \frac{V_E}{(1+i)^j} - (I_T + \sum_{j=1}^{y} \frac{C_O}{(1+i)^j})$$ relaţia (5.11)

Unde:

- VAN este valoarea actualizată netă pentru programul supus analizei
- y reprezintă numărul de ani constând în durata proiectului
- V_E reprezintă venituri anuale estimate aferente programului
- i reprezintă rata de actualizare folosită pentru calculul factorului de rentabilitate
- I_T reprezintă investiţiile totale ale programului
- C_O reprezintă costurile operaţionale anuale aferente programului

Pe baza valorii actualizate netă, se calculează factorul de rentabilitate ca fiind:

$$F_R = \begin{cases} 0, dacă\ VAN < 0 \\ 1, dacă\ VAN > 0 \end{cases}$$, relaţia (5.12)

Unde:

- F_R reprezintă factorul de rentabilitate al programului
- VAN este valoarea actualizată netă pentru programul supus analizei

În vedere evaluării unui termen economic specific domeniului investiţional, şi anume rata internă a rentabilităţii, folosim următoarea formulă:

$$RIR = i_{min} + (i_{max} - i_{min}) \cdot \frac{VAN_+}{VAN_+ - VAN_-}$$, relaţia (5.13)

Unde:

- RIR este valoarea ratei interne de rentabilitate a investiţiei supusă analiză
- VAN_+ reprezintă valoarea actualizată netă pozitivă
- VAN_- reprezintă valoarea actualizată netă negativă
- $i_{\min}$ reprezintă rata de actualizare folosită pentru calculul VAN_+
- $i_{\max}$ reprezintă rata de actualizare folosită pentru calculul VAN_-

6. IMPLEMELENTAREA TEHNICILOR DE AUDIT ÎN PROCESUL DE MIGRARE CĂTRE ARHITECTURI CLOUD

6.1 ARHITECTURA GENERALĂ A PROCESULUI DE MIGRARE

Pentru validarea metodologiei propusă pentru procesul de audit al migrării în cloud, am folosit următoarea arhitectură:

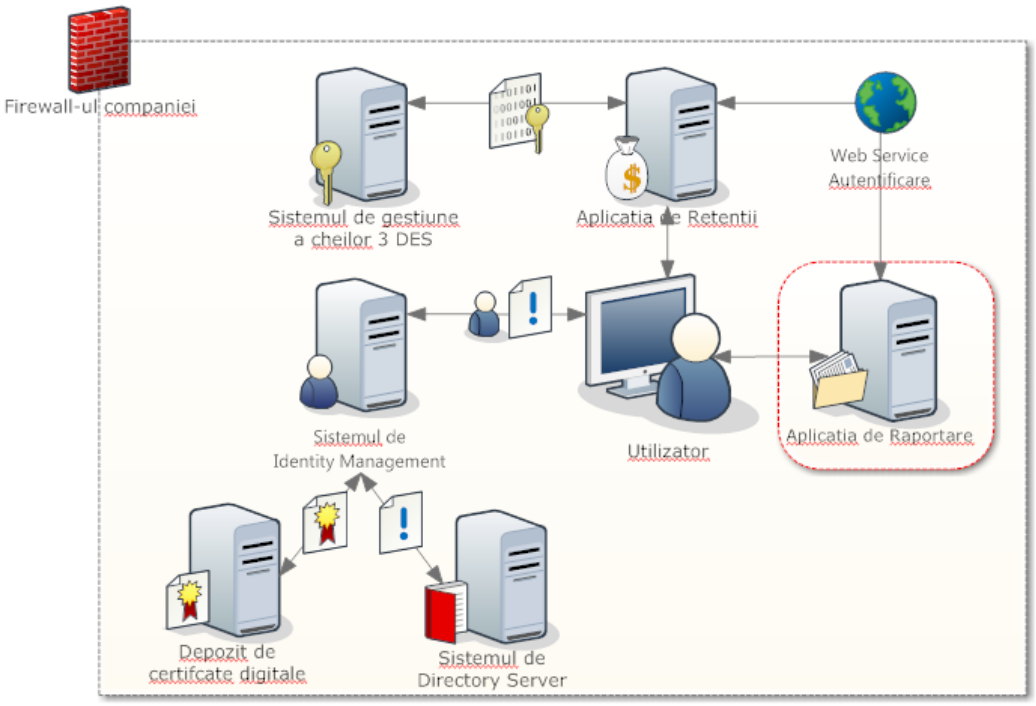

Fig. 6.1: Arhitectura Studiului de caz

Aplicaţia de raportare, supusă evaluării migrării, comunică cu sursele adiacente de date prin intermediul internetului. În urma analizei necesităţilor de performanţă, am evaluat caracteristicile de sistem pe care aplicaţia de raportare îmbunătăţită ar trebui să le aibă pentru a răspunde eficient solicitărilor, fie că sunt contractate de la furnizorul de cloud, fie că este îmbunătăţit sistemul intern. Aceste caracteristici sunt prezentate în tabelul următor:

Tabelul 6.1: Caracteristici necesare ale aplicaţiei de raportare

Nr	Nume caracteristică	Valoare dorită
1	Tip Aplicaţie	Web based
2	Număr de utilizatori	1500
3	Număr mediu de utilizatori concurenţi	10
4	Sistem de Operare	Linux x86 – RedHat 5
5	Putere de calcul	2.7 GHz
6	Memorie RAM	32 GB
7	Spaţiu de stocare	1 TB
8	Depozit de date	Oracle DB
9	Număr de Surse adiacente de date	10

Nr	Nume caracteristică	Valoare dorită
10	Versiune Serviciu Apache	2.4.7
11	Versiune Serviciu MySQL	5.5.34
12	Mecanism de autentificare	Sistemul de Identity Management
13	Volum de Date mediu tranzacţionate / zi	20 GB
14	Conexiune la internet	100 Mbps

6.2 RAPORTUL DE AUDIT AL PROCESULUI DE MIGRARE

În urma efectuării procesului de audit pentru aplicaţia de raportare, s-au obţinut următoarele valori:

Tabelul 6.2: Impactul migrării

Nr	Factor	Simbol	Valoare
1	Impactul migrării	i_{gen}	0.638379205
2	Impactul migrării către arhitecturi cloud de tip public	i_{pbc}	0.638379205
3	Impactul migrării către arhitecturi cloud de tip hibride	i_{hc}	0.713576159
4	Impactul migrării către arhitecturi cloud de tip interne	i_{pc}	0.756637168
5	Impactul migrării către arhitecturi interne	i_{id}	0.903474903

Reprezentarea grafică a factorilor de impact:

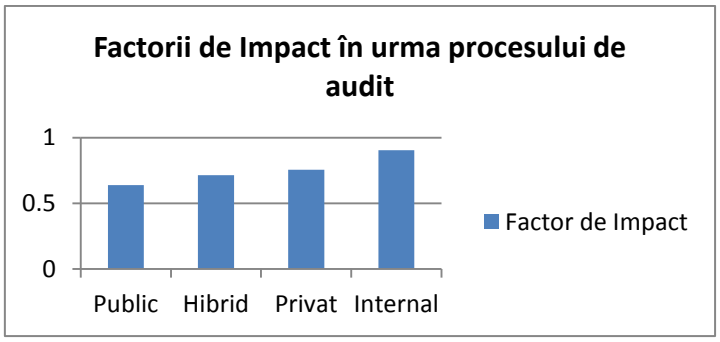

Fig. 6.2: Factorii de impact obţinuţi în procesul de audit

În urma analizei realizate, s-a constat că migrarea către o infrastructură de tip cloud a aplicaţiei de raportare este oportună, fapt indicat şi de factorul de valoare obţinut de arhitecturile cloud computing în detrimentul implementării interne:

$$\varphi_{cloud} = 24\%, \text{ relaţia (6.1)}$$

Decizia de companiei a fost cea de adopţie a unei arhitecturi de tip public cloud, pe model de Infrastructure as a Service deoarece aplicaţia migrată este implementată, astfel încât îmbucăţirile care trebuie să i se aducă vizează doar performanţele şi costul.

6.3 CONCLUZII

Această implementare a fost realizată în vederea validării mecanismului de auditare a migrării unei aplicaţii existente în interiorul unei companii, către arhitecturi de tip cloud

computing. În urma procesului de audit am observat un rezultat pozitiv, în sensul obţinerii factorului de impact minim pentru modelul de livrare Infrastructure as a Service într-o arhitectură de cloud public – ceea ce demonstrează utilitatea modelului cloud în acest scenariu, iar furnizorul de cloud recomandat pe motive de rentabilitate şi fiabilitate a fost Amazon. Am putut demonstra astfel eficienţa mecanismului de evaluare al procesului de migrare. Acesta prezintă următoarele avantaje:

- Metodologia de audit oferă un mediu de evaluare al impactului migrării către soluţii de tip cloud, plecând de la practicile existente în comunităţile cloud, compensând astfel procese de evaluare costisitoare
- Algoritmul de calcul al factorului de impact este bazat atât pe experienţa existentă în procesele de migrare cât şi pe interdependenţa dintre întrebări
- Procesul de audit oferă companiei un raport clar şi uşor de citit cu privire la riscurile implicate de procesul de migrare şi acţiunile care pot fi întreprinse în vederea adresării şi diminuării lor.

După evaluarea factorului de risc şi luarea deciziei de migrare, procesul de audit a continuat cu expunerea etapelor principale ale procesului de adopţie. Acesta cuprinde, pe lângă activităţi clare premergătoare migrării în cloud şi o serie de best practice-uri de care compania trebuie să ţină cont pentru a spori adaosul de valoare adus de contractarea serviciilor cloud.

7. IMPLEMENTAREA TEHNICILOR DE AUDIT AL ARHITECTURILOR CLOUD

7.1 ARHITECTURA GENERALĂ PROCESULUI DE AUDIT

Infrastructura în care am realizat acest studiu de caz include:

- Aplicaţia de Identity Management[20]
- Sistemul de Federalizare de Identităţi şi Single Sign On[21]
- Directory Server[22]
- Sistem de criptare a traficului[23]
- Salesforce.com – acest sistem este cel supus analizei.

Caracteristicile programului de implementare ale aplicaţiei salesforce.com sunt:

Tabelul 7.1: Caracteristici ale aplicaţiei supusă procesului de auditare a migrării în cloud

Nr	Nume caracteristică	Valoare
1	Nume aplicaţie	Salesforce.com
2	Aplicaţie Sensibilă	Nu
3	Nivel de Risc Asumat	2
4	Nume Proiect de implementare	Salesforce
5	Nume Program de implementare	Salesforce
6	Durata Programului	7 ani
7	Durata de implementare	1 an
8	Nivelul de maturitate aşteptat	3
9	Venituri medii anuale estimate	100.000 €
10	Investiţie totală	300.000 €
11	Durată investiţie	1 an
12	Cost operational anual	10.000 €
13	Cost investiţie	10%
14	Tipul de serviciu cloud	SaaS
15	Modelul cloud	Cloud Public

Datele prezentate în tabelul de mai sus reprezintă date de intrare pentru algoritmul de calcul al factorilor de siguranţă şi de rentabilitate.

7.2 Rezultatele procesului de auditare

Factorul de Siguranţă

Rezultatele procesului de audit sunt sumarizate în tabelul următor:

Fig. 7.1: Rezultatele procesului de audit al aplicaţiei salesforce.com din perspectiva siguranţei

Domeniu	Număr de controale	Riscul Aplicaţiei	Riscul Asumat	Factorul de Siguranţă
Governance and Enterprise Risk Management	41	0.65	0.82	0.982266508
Traditional Security, Business Continuity and Disaster Recovery	17	0.18	0.34	0.977543253

[20] Sistemul care provizionează conturi în aplicaţia salesforce.com.
[21] Acest sistem este folosit pentru procesul de autentificare al utilizatorului în salesforce.com.
[22] Acest sistem este sursa de date a sistemului de Identity Management.
[23] Acest sistem se află în DMZ. El criptează toate datele transmise din interiorul companiei către salesforce.

Domeniu	Număr de controale	Riscul Aplicaţiei	Riscul Asumat	Factorul de Siguranţă
Compliance and Audit	40	0.41	0.8	0.984875
Portability and Interoperability	8	0.14	0.16	0.94625
Incident Response, Notification and Remediation	17	0.35	0.34	0.965778547
Application Security	12	0.23	0.22	0.951983471
Encryption and Key Management	33	0.67	0.66	0.977695133
Identity and Access Management	62	0.7	1.22	0.986237571
Virtualization	10	0.11	0.2	0.968
Data Center Operations	17	0.13	0.34	0.98100346
Information Management and Data Security	5	0.01	0.1	0.982
Total Controale	262	Factorul de Siguranţă General		0.97305754

Aşa cum se poate observa, domeniile în care s-a depăşit gradul de risc asumat sunt:

- Incident Response, Notification and Remediation
- Application Security
- Encryption and Key Management

Din perspectiva factorului de siguranţă, acesta a variat de la 94.625% până la 98.623%, obţinându-se o medie de 97.305%, fapt ce recomandă salesforce.com ca un sistem sigur.

Figura de mai jos prezintă în mod grafic, factorii de siguranţă obţinuţi pentru fiecare domeniu în parte:

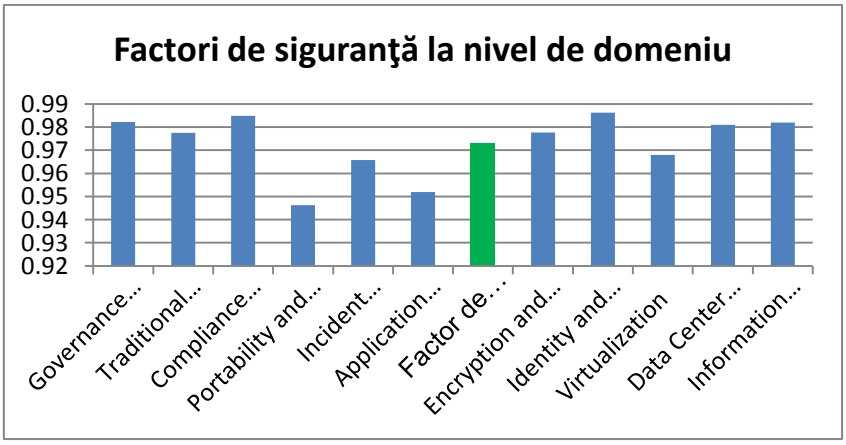

Fig. 7.2: Analiză comparativă între factorii de siguranţă obţinuţi

Factorii de conformitate pentru aplicaţia auditată în raport cu toate domeniile supuse analizei sunt:

- Governance and Enterprise Risk Management: $NC_1 \cong 0.98$
- Traditional Security, Business Continuity and Disaster Recovery: $NC_2 \cong 0.97$
- Compliance and Audit: $NC_3 \cong 0.98$
- Portability and Interoperability: $NC_4 \cong 0$
- Incident Response, Notification and Remediation: $NC_5 \cong 0.96$

- Application Security: $NC_6 \cong 0.95$
- Encryption and Key Management: $NC_7 \cong 0.97$
- Identity and Access Management: $NC_8 \cong 0.98$
- Virtualization: $NC_9 \cong 0.96$
- Data Center Operations: $NC_{10} \cong 0.98$
- Information Management and Data Security: $NC_{11} \cong 0.98$

Figura de mai jos prezintă rezultatele în mod grafic:

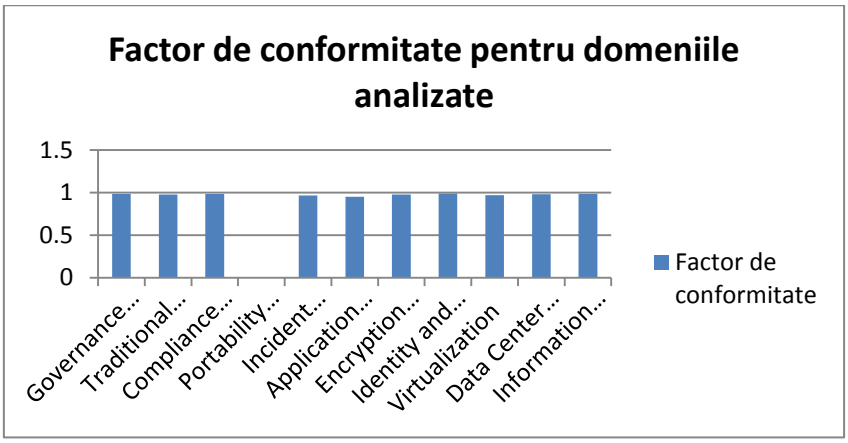

Fig. 7.3: Factori de conformitate ai domeniilor analizate în raport cu standardele folosite

Se poate concluziona că, aplicaţia salesforce.com este conformă cu cerinţele de securitate care definesc o aplicaţie ca fiind sigură în 10 din cele 11 domenii analizate. Domeniul neconform este Portability and Interoperability. Analizând mecanismele de control ale acestui domeniu s-a constatat că interoperabilitatea cu alte sisteme este asigurată, însă la domeniul portabilitate salesforce.com trebuie să aducă îmbunătăţiri.

Din perspectiva factorului de siguranţă, raportul de audit a recomandat îmbunătăţirea controalelor din următoarele domenii:

- Portability and Interoperability
- Application Security

Factorul de rentabilitate

Tabelul de mai jos prezintă scorurile de maturitate obţinute pe fiecare domeniu ValIT analizat:

Tabelul 7.2:Nivelurile de maturitate al programului Salesforce rezultate în urma auditului

Domeniu	Grad de Maturitate
Value Governance (VG)	3
Portfolio Management (PM)	3.666666667
Investment Management (IM)	3
Total	3.222222222

Valoarea Actualizare Netă obţinută în analiza factorului de rentabilitate a fost ulterior folosită în calcularea următorului indice economic, cel al ratei interne de rentabilitate.

Tabelul de mai jos reprezintă în mod schematic datele utilizate pentru calculul Valoarea Actualizare Netă pentru programul auditat:

Tabelul 7.3: Datele financiare ale programului Salesforce

	Investiţii	Cheltuieli	Venituri
Anul 1	300000		
Anul 2		7971.938776	79719.38776
Anul 3		7117.802478	71178.02478
Anul 4		6355.180784	63551.80784
Anul 5		5674.268557	56742.68557
Anul 6		5066.311212	50663.11212
Anul 7		4523.492153	45234.92153
Venituri Totale		367089.9396	
Cheltuieli Totale		336708.994	
VAN		30380.94564	

Pentru calcularea valorii negative a Valorii Actualizate Anuală necesară pentru estimarea ratei interne de rentabilitate am crescut rata de actualizate cu 0.03, obţinând rezultatele prezentate în tabelul de mai jos:

Tabelul 7.4: Datele financiare folosite în calculul rentabilităţii

	Investiţii	Cheltuieli	Venituri
Anul 1	300000		
Anul 2		7561.436673	75614.36673
Anul 3		6575.162324	65751.62324
Anul 4		5717.532456	57175.32456
Anul 5		4971.767353	49717.67353
Anul 6		4323.275959	43232.75959
Anul 7		3759.370399	37593.70399
Venituri Totale		329085.4516	
Cheltuieli totale		332908.5452	
VAN		-3823.093519	

Se poate observa astfel că veniturile se diminuează considerabil, fapt ce duce la o Valoare Actualizată Netă negativă.

Folosind aceste valori, am calculate rate internă de rentabilitate:

$RIR \cong 14\%$, relaţia (7.1)

Considerând că dobânda medie anuală la băncile din România este de 6 % pe an, programul Salesforce a reuşit, conform ratei interne de rentabilitate prezentată mai sus, să valorifice investiţiile realizate cu o eficienţă mai mult decât dublă decât scenariul în care investiţiile erau păstrate în bancă, fapt ce o califică drept o investiţie profitabilă.

7.5 CONCLUZII

Acest studiu de caz a fost realizat în vederea validării mecanismului de auditare a soluţiilor cloud propuse în capitolul 5 al acestei lucrări.

Sumarizând rezultatele procesului de audit, putem concluziona următoarele aspecte:

- Aplicaţia salesforce.com implementată în arhitectura descrisă în secţiunea 7.1 prezintă un factor de siguranţă de 97% fapt ce o califică drept o aplicaţie stabilă
- Aplicaţia salesforce este conformă cu standardele folosite pentru analizarea acesteia în 10 din cele 11 domenii ale sale, media gradului de conformitate pe aceste 10 domenii fiind de 97.7%.
- Gradul de conformitate din perspectiva tuturor domeniilor este de 90.9% tradus în faptul că 10 din cele 11 domenii de securitate analizate au avut factor de siguranţă mai mare sau cel puţin egal cu 95%. Domeniul neconform a avut un factor de siguranţă 94.62% ceea ce înseamnă că efortul pentru a deveni conform nu este semnificativ.
- Programul de implementare al aplicaţiei supusă auditului a depăşit nivelul de maturitate aşteptat, ceea ce demonstrează gradul de adaptabilitate crescut al companiei la schimbare, precum şi tendinţa de acomodare rapidă şi eficientă cu abordarea oferită de arhitecturile cloud.

Aşadar putem concluziona că, salesforce.com este o poveste de succes în compania supusă analizei, care poate fi invocată în vederea susţinerii dezvoltării strategie de inovaţie în departamentul IT către arhitecturi de tip cloud computing.

CONCLUZII

C.1. CONCLUZII GENERALE

Procesul de audit este cel care asigură compania că a luat decizia corectă pentru infrastructura IT şi mediul de business în care acesta activează de migrare către un anumit model de cloud, prin adresarea aspectelor relevante acelei arhitecturi şi evaluarea caracteristicilor specifice ale aplicaţiei sau sistemului suspus migrării. Prima componentă de audit prezentată în această lucrare demonstrează rolul fundamental al auditului chiar din faza incipientă a procesului de adopţie, aducând următoarele avantaje care fac diferenţa între o decizie corectă şi una incorectă:

- Auditul de evaluare al procesului de migrare către arhitecturi de tip cloud oferă vizibilitate în cadrul companiei
- Auditul de evaluare al procesului de migrare către arhitecturi de tip cloud oferă o analiză specifică pe sistemul respectiv

În ceea ce priveşte evaluarea serviciilor cloud, aceasta este adresată tot de către componenta de audit, însă de această data, din alte perspective. Aşadar o altă direcţie de cercetare pe care am urmat-o a vizat stabilirea unui framework de auditare a componentelor cloud pentru a oferi o cuantificare a riscului legate de cloud.

În încheierea acestei secţiuni de concluzii, vreau să reiterez faptul că, fenomenul Cloud Computing este, cu siguranță, una dintre cele mai ispititoare arii tehnologice din zilele noastre atât datorită costurilor reduse pe care le implică cât și datorită flexibilității de care dă dovadă.

C.2. CONTRIBUȚII ORIGINALE

Scopul cercetării mele a fost acela de a veni în întâmpinarea necesităţii unei companii de a răspunde prezent acestui nou concept – cloud. Plecând de la această idee, am căutat un mod eficient de adresa toate neajunsurile, riscurile și provocările acestui domeniu. Activitatea mea s-a desfășurat pe trei direcții mari:

- Procesul de evaluare al adopției arhitecturilor cloud computing
- Integrarea sistemelor în arhitecturi hibride
- Procesul de auditare al serviciilor cloud

În domeniul ce vizează auditul procesului de migrare către arhitecturi de tip cloud, am implementat o nouă abordare de tratare a unui proces de migrare ce mi-a permis:

- Cuantificarea factorului de risc al migrării aplicației cloud şi a surplusului de valoare adus de arhitecturile cloud
- Analiza comparativă a factorilor de risc asociați cu diferitele modele de cloud

Pentru validarea acestei abordări am realizat o implementare care a demonstrat utilitatea aportului meu în analizarea perspectivei de migrare.

Cercetarea mea a continuat în acest domeniu, cu analiza interacţiunii dintre sistemele din interiorul companiei şi cele din cloud şi am realizat două modele de abordare a unor problematici stringente din domeniul cloud:

- Comunicaţia între un sistem intern de date care stochează informaţii confidenţiale a căror stocare nu se poate migra către cloud
- Extinderea conceptului de Identity Management de la nivelul companiei la nivel arhitectural logic, extinzând practic graniţele companiei în internet.

Pentru adresarea primei problematici am realizat un proces eficient care manipulează date confidenţiale criptat, asigurând că decriptarea se face în condiţii sigure de autentificare şi autorizare.

Prin metodologia realizată am obţinut următoarele beneficii:

- Toate datele confidenţiale sunt stocate criptate, chiar şi cele din interiorul companiei
- Există trei mecanisme folosite pentru asigurarea AAA
- Chiar dacă există un eveniment de atac soldat cu accesul neautorizat la datele stocate în aplicaţia migrate în cloud, atacatorul nu va putea dispune de aceste informaţii întrucât al doilea mecanism de autentificare a utilizatorului final va eşua şi datele nu vor putea fi decriptate

Am realizat o abordare eficientă a aspectelor legate de Identity Management prin creşterea gradului de complexitate în autentificarea utilizatorilor la sistemele cloud. Principalele beneficii ale acestei abordări sunt:

- Utilizatorul nu îşi poate altera drepturile de acces la aplicaţia cloud
- Există un proces cu 2 paşi de verificare contra furtului de certificate digitale
- Procesul de autentificare implică mai multe sisteme, fapt ce face imposibil un atac de tipul *man in the middle* cu un singur pas de penetrare.
- Identitatea digitală conţine doar informaţiile necesare serviciilor din aplicaţia cloud care îi sunt permise utilizatorului
- Identitatea digitală este distrusă după ce este folosită, fără a fi stocată în aplicaţia cloud
- Propunerea unui algoritm eficient de criptare a traficului sensibil.

În domeniul auditului aplicaţiilor cloud computing, am realizat o metodologie de audit eficientă care să ofere o cuantificare măsurilor de siguranţă.

Principalele contribuţii în acest domeniu ale abordării mele constau în:

- Propunerea unui algoritm eficient de stabilire a factorului de siguranţă ce ia în calcul toţi factorii contextuali ai procesului de audit
- Evaluarea principalelor mecanisme de control al securităţii
- Cuantificarea guvernanţei şi securităţii aplicaţiei analizate prin factorul de siguranţă şi a conformităţii cu standardele folosite

Abordarea personală a procesului de audit al soluţiilor de cloud computing cuprinde şi un al doilea sub-domeniu care adresează componenta economică a strategii şi gradul de maturitate pe care procesele de guvernanţă şi gestiune a programelor în această arie arhitecturală îl au, care oferă următoarele beneficii:

- Propunerea unui algoritm eficient de stabilire a factorului de rentabilitate
- Evaluarea unui program din cadrul companiei pentru stabilirea strategiei companiei, fapt ce oferă suport decizional în privinţa alegerii direcţiei de dezvoltare
- Analiza completă a programului de implementare al soluţiei cloud, fapt ce oferă posibilitatea evidenţierii domeniilor celor mai mature şi a acelora în care trebuie aduse îmbunătăţiri. Această analiză poate sta la baza deciziile strategice de guvernanţă şi management al riscului din companie

Pentru validarea metodologiei originale prezentate, am realizat o implementare care analiza soluţia salesforce.com într-o arhitectură specifică atât din perspectiva factorului de siguranţă cât şi din perspectiva factorului de rentabilitate.

C.3 DISEMINAREA REZULTATELOR

Lista de lucrări prezentate la conferinţe internaţionale:

1. *G. Mateescu, M. Vlădescu, V. Sgârciu*, The Design and Implementation of an Experimental Model for Secure Management of Personal Data Based on Electronic Identity Card and PKI Infrastructure, 2012, 14th IFAC Symposium on Information Control Problems in Manufacturing, INCOM
2. *G. Mateescu, M. Vlădescu, V. Sgârciu*, The Design and Validation of an Experimental Model for the Secure and Efficient Medical Services based on PKI Infrastructures and Smart-Cards, 2012, 14th IFAC Symposium on Information Control Problems in Manufacturing, INCOM
3. *G. Mateescu, M. Vlădescu,* A hybrid approach of system security for small and medium enterprises: Combining different cryptography techniques , 2013, Computer Science and Information Systems (FedCSIS)
4. *Georgiana Mateescu, Marius Vlădescu,* Secure On Premise - On Demand Services Communication, 2013 , System Theory, Control and Computing (ICSTCC), 2013 17th International Conference, ISBN 978-1-4799-2227-7
5. *Georgiana Mateescu, Marius Vlădescu,* Identity Management Approach for Software as a Service, 2013, The Eighth International Conference on Systems and Networks Communications, ICSNC 2013

Lista de lucrări publicate în reviste:

6. *Georgiana Mateescu, Marius Vlădescu* – Auditing Hybrid IT Environments - International Journal of Advanced Computer Science and Applications (http://thesai.org/Publications/IJACSA) – Aprilie 2014

Lista de lucrări în curs de publicare:

7. *Georgiana Mateescu, Marius Vlădescu,* Identity Management Approach for Software as a Service [versiunea extinsă] - International Journal On Advances in Software (IARIA Journals), 2014
8. *Georgiana Mateescu, Valentin Sgârciu*, Cloud Computing Audit – Scientific Bulletin UPB (Submission ID 2801), 2014
9. *Georgiana Mateescu, Marius Vlădescu, Valentin Sgârciu*, Auditing Cloud Computing Migration - IEEE 9th International Symposium on Applied Computational Intelligence and Informatics, SACI 2014

Lista de lucrări trimise spre publicare:

10. *Marius Vlădescu, Georgiana Mateescu, Valentin Sgârciu*, Security measures for laptop loss or theft in enterprises, - 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, AQTR
11. *Georgiana Mateescu, Marius Vlădescu, Valentin Sgârciu*, Addressing Identity Management in Cloud Computing Architectures - 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, AQTR
12. *Marius Vlădescu, Georgiana Mateescu, Valentin Sgârciu*, Event Correlation for enterprise internal security - 7th International Conference on Security for Information Technology and Communications – SECITC'14
13. *Georgiana Mateescu, Marius Vlădescu, Valentin Sgârciu*, - Holistic approach to evaluate the cloud adoption 7th International Conference on Security for Information Technology and Communications – SECITC'14

C.3. PERSPECTIVE DE DEZVOLTARE ULTERIOARĂ

Perspectivele de dezvoltare ulterioară a contribuţiilor personale în domeniului auditului în cloud vizează particularizarea şi specializarea abordărilor propuse pe arii şi industrii specifice.

BIBLIOGRAFIE SELECTIVĂ

[1] *Rajkumar Buyya, James Broberg and Andrzej M. Goscinski*, Cloud Computing: Principles and Paradigms, 2011, John Wiley & Sons ISBN:9780470887998

[2] *Wim Van Grembergen, Steven De Haes,* Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value, 2008 , Springer ISBN:9780387848815

[3] *George Rees*, Cloud Application Architectures, 2009, O'Reilly Media, ISBN:978-0-596-15636-7

[4] *Anca Daniela Ionita, Marin Litoiu, Grace Lewis*, Migrating Legacy Applications: Challenges in Service Oriented Architecture and Cloud Computing Environments, 2013, IGI Global, ISBN:9781466624887

[5] *Jatinder N. D. Gupta, Sushil K. Sharma*, Handbook of Research on Information Security and Assurance, 2009, IGI Global, ISBN:9781599048550

[6] *Irene Maria Portela, Maria Manuela Cruz-Cunha*, Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues, 2010, IGI Global,ISBN:9781615209750

[7] *ISACA,* COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, 2012, ISACA ISBN:9781604202373

[8] *Michael Workman, Daniel C. Phelps, John N. Gathegi*, Information Security for Managers, 2013, Jones and Bartlett Publishers ISBN:9780763793012

[9] *Cloud Security Alliance*, Security Guidance for critical areas of focus in cloud computing v3.0, 2011 https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[10] *Xiaoyu Yang, Lu Liu*, Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing, 2013, IGI Global,ISBN:9781466628540

[11] *Robert R. Moeller,* Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL, 2013 John Winley & Sons ISBN:9781118138618

[12] *Nick Antonopoulos, Lee Gillam*, Cloud Computing: Principles, Systems and Applications, 2010, Springer ISBN:9781849962407

[13] *Siani Pearson, George Yee* , Privacy and Security for Cloud Computing, 2013, Springer ISBN:9781447141884

[14] *Paul Brant, Denis Guyadeen,* How to Trust the Cloud: "Be Careful Up There", 2010, EMC

[15] *Ian Lim, E. Coleen Coolidge, Paul Hourani*, Securing Cloud and Mobility: A Practitioner's Guide, 2013, Auerbach Publications, ISBN:9781439850558

[16] *Craig Gentry*, A fully homomorphic encryption scheme, 2009, Phd Thesis

[17] *Chris Davis, Mike Schiller, Kevin Wheeler*, IT Auditing: Using Controls to Protect Information Assets, Second Edition, 2011 McGraw-Hill/Osborne ISBN:9780071742382

[18] *Xiaoyu Yang, Lu Liu*, Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing, 2013, IGI Global,ISBN:9781466628540

[19] *ISACA,* Cloud Computing Management Audit/Assurance Program, 2010

[20] *ISACA,* Identity Management Audit/Assurance Program, 2009, ISACA

[21] *Kurt J. Engemann and Douglas M. Henderson,* Business Continuity and Risk Management: Essentials of Organizational Resilience, 2012, Rothstein Associates ISBN:9781931332545