CECCAR BUSINESS REVIEW
ISSN 2668-8921 • ISSN-L 2668-8921
Nº 2/2020
www.ceccarbusinessreview.ro

Modelul COSO al controlului intern
– partea a II-a –

Conf. univ. dr. Mirela PĂUNESCU
ASE București

Abstract

The main purpose of internal control is to provide reasonable assurance regarding the achievement of the entity's general objectives (regardless of whether the entity is a trading company or not). A core prerequisite of an effective internal control is to have clear objectives set by the company's management.

Two internal control models have gained international recognition: the COSO Model and the CoCo Model. This article discusses the former.

Key terms: control environment, risk assessment, control activities, information, communication, monitoring

Termeni-cheie: mediul de control, evaluarea riscurilor, activități de control, informare, comunicare, monitorizare

Clasificare JEL: G39

To cite this article: Mirela Păunescu, *Modelul COSO al controlului intern (II)*, *CECCAR Business Review*, Nº 2/2020, pp. 40-46, DOI: http://dx.doi.org/10.37945/cbr.2020.02.05

➲ Activitățile de control privind tehnologia informațiilor

În prezent este greu de imaginat viața fără tehnologie. În companiile mari, din ce în ce mai multe activități se bazează pe aceasta. Sunt sisteme integrate care facturează, trimit e-mailuri de notificare privind întârzierile la plată, înregistrează tranzacțiile în contabilitate, fac confirmările cu terții în mod automatizat și multe altele. Tehnologia dă dependență. Roboții preiau din ce în ce mai mult din responsabilitățile oamenilor. Tehnologia are un rol extrem de benefic în dezvoltarea entității, dar vine la pachet cu niște riscuri.

Ca un scurt exemplu, inclusiv verificările informațiilor provenite din utilizarea tehnologiei trebuie făcute diferit față de cele prelucrate de oameni, deoarece riscurile sunt diferite. Concret, dacă algoritmul de calcul al totalului este verificat și este corect, cu excepția situației în care cineva intervine în sistemul informatic și îl denaturează, toate totalurile vor fi determinate corect. Calculatorul nu obosește, nu este distras, nu are vacanță, nu este neatent. Dacă însă algoritmul din spatele prelucrării este eronat, cu siguranță totalurile vor fi sistematic greșite (eroarea este repetitivă și, deși poate fi nesemnificativă în mod individual, ea poate deveni importantă prin agregare și repetiție).

Ca atare, în ultima perioadă s-a pus accentul pe acele activități de control care pot fi implementate cu ajutorul tehnologiilor și care asigură că tehnologia funcționează așa cum a fost concepută, fără a permite manifestarea riscurilor specifice (cunoscute și ca riscuri cibernetice – *cyber risks*).

Acestea includ riscuri:

- de securitate;

- de siguranță;
- de arhivare (stocare);
- de procesare a informațiilor;
- care țin de componentele hardware și software;
- legale etc.

Controalele privind tehnologia informațiilor sunt diferite de cele explicate anterior și pot fi clasificate în două mari grupe, respectiv:

■ Controale generale

Potrivit ISA 315 *Identificarea și evaluarea riscurilor de denaturare semnificativă prin înțelegerea entității și a mediului său*, controalele generale sunt politici și proceduri care se aplică tuturor sau unui segment larg al sistemelor informatice ale instituției (cum ar fi sistemele *mainframe*, microcalculatoarele, rețelele și utilizatorii finali) și care contribuie la asigurarea funcționării lor corespunzătoare, constituind mediul de operare a sistemelor și controalelor de aplicații.

Principalele categorii sunt:

- administrarea și planificarea programului de securitate la nivel de instituție – asigură un cadru și un ciclu continuu de activitate pentru riscul de management, creând politici de securitate, atribuind responsabilități și monitorizând conformitatea controalelor aferente calculatoarelor instituției;
- controalele de acces – limitează sau detectează accesul la resursele calculatoarelor (date, programe, echipamente și facilități), protejând respectivele resurse împotriva modificărilor neautorizate, pierderilor sau accesărilor și distribuirilor neautorizate. Controalele de acces le includ atât pe cele fizice, cât și pe cele logice;
- controalele privind dezvoltarea, menținerea și modificarea softului de aplicații – previn modificările neautorizate ale programelor existente;
- controalele softului sistemelor – limitează și monitorizează accesul la programele și fișierele sensibile care controlează sistemul hardware al calculatoarelor și asigură funcționarea aplicațiilor suportate de sistem;
- separarea sarcinilor – de o manieră similară cu cele aplicabile tranzacțiilor manuale, aceste controale presupun instituirea politicilor, procedurilor și structurii organizatorice care să prevină verificarea de către o persoană a tuturor aspectelor-cheie ale operațiunilor informatice și, în consecință, efectuarea de operațiuni neautorizate sau obținerea de acces neautorizat la active ori evidențe;
- continuitatea serviciului – asigură, în situații de producere a unor evenimente neașteptate, continuarea fără întrerupere sau reluarea promptă a operațiunilor critice și protejarea datelor critice sau sensibile.

Câteva exemple de controale generale ale sistemelor IT sunt cele care permit modificarea programelor doar în anumite condiții, cele care restricționează accesul la programe sau date (doar persoanele autorizate le pot accesa), controalele implementării noilor versiuni ale aplicațiilor software sau controalele software-ului de sistem care restricționează accesul la sau monitorizează folosirea utilităților sistemului.

■ Controale de aplicații

Controalele de aplicații se referă la politica și procedurile care vizează sistemele de aplicații individuale, separate (spre exemplu, cele aplicabile modulului de salarizare sau de facturare), și au drept scop acoperirea procesării datelor în cadrul softului de aplicații specific. Aceste controale sunt create pentru a preveni, depista sau corecta erorile din fluxurile de informații în sistemele informatice.

Controalele de aplicații pot fi clasificate în funcție de mai multe criterii.

Astfel, în funcție de momentul în care sunt aplicate, ele se pot urmări în trei faze ale ciclului de procesare:

- controale aplicate la intrare – verifică dacă datele sunt autorizate, convertite în format automatic și introduse în aplicație în mod corect, complet și oportun;
- controale aplicate la procesare – verifică dacă datele sunt procesate în mod adecvat de calculator și dacă fișierele sunt actualizate corect;
- controale aplicate la ieșire – verifică dacă fișierele și rapoartele generate de aplicație reflectă tranzacțiile sau evenimentele care s-au produs efectiv, evidențiind corect rezultatele procesării, și dacă rapoartele sunt controlate și distribuite utilizatorilor autorizați.

În funcție de tipurile de obiective de control aferente, ele pot fi:

- controale de autorizare – privesc valabilitatea tranzacțiilor și oferă asigurarea că acestea reprezintă evenimente care au avut într-adevăr loc într-o perioadă dată. Spre exemplu, sistemul informatic refuză emiterea unei facturi cu o dată incorectă (din trecut sau din viitor) ori înregistrarea unui salariat dacă el nu este găsit în baza de date cu salariații aprobați de departamentul de resurse umane;
- controale de integralitate – verifică dacă toate tranzacțiile valabile sunt înregistrate și clasificate corespunzător. Spre exemplu, un sistem informatic poate raporta că există livrări de bunuri care nu au fost facturate sau facturi emise care nu au fost înregistrate în contabilitate;
- controale de corectitudine – verifică dacă tranzacțiile sunt înregistrate corect și dacă toate datele sunt precise.

În literatura de specialitate putem găsi și alte tipuri de clasificări ale controalelor de aplicații.

Controalele de aplicații depind în mare măsură de eficiența controalelor generale. Dacă acestea din urmă sunt ineficiente, siguranța controalelor privind aplicațiile individuale este afectată. Spre exemplu, degeaba există controale privind aplicația de calcul, plată și raportare a salariilor dacă cineva din exterior poate veni și accesa sistemul nefiind autorizat.

Controalele generale și cele de aplicații sunt interconectate, ambele fiind necesare pentru a asigura o procesare corectă și completă a informațiilor. Foarte important este să subliniem din nou faptul că, oricât de eficiente ar fi, controalele privind tehnologia informațiilor pot oferi conducerii doar o asigurare rezonabilă, și nu una absolută, în legătură cu informațiile procesate de sistemele informatice, și anume că acestea îndeplinesc obiectivele de control preconizate (asigurarea integralității, oportunității și valabilității datelor și păstrarea integrității acestora).

În ceea ce privește controalele relevante pentru raportarea financiară, exemplele de controale ale aplicațiilor includ verificarea exactității matematice a înregistrărilor, menținerea și revizuirea conturilor și balanțelor de verificare, controalelor automate precum validările editărilor privind datele de intrare și verificările secvențelor numerice, urmărirea manuală a rapoartelor de excepție etc.

Exemplul 1

■ **Barings Bank**

Până la dispariția sa (la venerabila vârstă de 233 de ani, în 1995), Barings Bank a fost cea mai veche bancă comercială din Anglia (fusese fondată în anul 1762). Banca Barings a fost cumpărată în 1995 de banca olandeză ING pentru suma totală de o liră sterlină. Dar, deși prețul pare tentant pentru oricare dintre noi (cine nu și-ar permite o bancă la prețul de o liră!), ING și-a asumat și toate datoriile băncii preluate. Ulterior, activele acesteia au fost divizate și vândute de către ING.

Cauza prăbușirii băncii se pare că a fost un broker din Singapore, Nick Leeson, responsabil cu arbitrajul între cotațiile futures Nikkei din Singapore și Osaka. Depășindu-și cu mult mandatul și nefiind oprit de nimeni și de nimic, Leeson a decis să parieze pe evoluția Nikkei 225 folosind contracte futures și opțiuni. Din păcate, în ciuda unor rezultate pozitive anterioare raportate de broker, pierderea totală generată a fost de 1,4 miliarde de dolari.

Se pare că motivul principal care a permis acumularea unor pierderi uriașe în numele băncii a fost lipsa controlului intern și a supravegherii. În mod evident, dacă ar fi existat mecanisme de control intern implementate și funcționale (cum ar fi aprobări relevante, monitorizarea în timp real a pierderilor în creștere, supravegherea activității de către responsabili etc.), operațiunile neautorizate ale brokerului ar fi fost posibil de identificat și stopat până să ajungă în acel punct în care nu s-a mai putut face nimic. În lipsa lor, brokerul s-a angajat în astfel de tranzacții mult peste limita lui de competență și a putut insista în privința lor (nedetectat și nederanjat de nimeni), deși la un moment dat era clar că pierderile acumulate sunt importante inclusiv pentru o bancă atât de mare cum era Barings. Cel mai probabil, Leeson a tot sperat că roata se va întoarce astfel încât pierderea să se transforme într-un câștig sau măcar să se diminueze semnificativ.

Aceste tipuri de tranzacții sunt deosebit de riscante, deoarece, în funcție de instrumentul în care se investește, investiția inițială este mică, dar pierderea poate fi nelimitată. Mai mult, pentru tranzacțiile cu instrumente financiare derivate trebuie determinată o valoare probabilă (valoare justă) a câștigurilor sau pierderilor anticipate, ceea ce face ca riscurile asociate acestora (de raportare financiară) să fie mari.

Concret, s-a consemnat că separarea sarcinilor nu era bine implementată în cazul Barings, în sensul că brokerul cumula mai multe responsabilități: era responsabil cu activitățile de tranzacționare și avea drept de semnătură și autorizare pentru tranzacții cu risc extrem de ridicat și reconcilieri bancare. Se pare că acesta a reușit să își ascundă pierderile de care era responsabil prin manipularea înregistrărilor într-un cont special. Suplimentar, norocosul Leeson nu avea vreo persoană responsabilă cu supravegherea sa, deși poziția lui în organigramă nu ar fi justificat un astfel de tratament. Managementul nu înțelegea pe deplin activitatea derulată de broker, motiv pentru care nu a identificat sumele și raportările neobișnuite.

Inacțiunea băncii este de neînțeles cu atât mai mult cu cât se pare că auditorii săi interni au raportat anterior aspecte neconforme cu normele impuse acesteia (cum ar fi cumularea de sarcini) și au recomandat separarea responsabilităților și monitorizarea activităților cu risc mare.

În urma scandalului, alte deficiențe majore ale controlului intern au fost raportate la Barings, printre care:

- nu existau restricții de tranzacționare;
- lipseau pârghiile/controalele de monitorizare, prevenire și identificare a activităților suspecte;
- nu avea implementat un sistem de identificare și evaluare a riscurilor;
- nu existau raportări privind eventualele riscuri identificate;
- nu se monitoriza activitatea angajaților (cu atribuții de tranzacționare, spre exemplu);
- nu avea stabilită o limită pentru sumele care puteau fi tranzacționate (de exemplu, nimeni nu a întrebat de ce are nevoie un broker de sume uriașe de bani zilnic pe o perioadă lungă);
- nu se monitorizau regulat indicatorii băncii (lichiditatea sau alți indicatori de risc care ar fi putut arăta că este ceva în neregulă);
- politica de recrutare a salariaților era ineficientă, în sensul că nu se cereau experiență și drept de practică (de tranzacționare);
- existau deficiențe în politica de training, în sensul că salariații nu beneficiau de cursuri relevante și utile în activitatea lor (specialiștii consideră că doar un broker începător și fără minimum de cunoștințe ar fi

putut să aleagă opțiunea de investiții pe care a decis-o Nick Leeson – același preț și aceeași dată de expirare –, deoarece era deosebit de riscantă și generatoare de pierderi mari);

- modul în care erau salarizați angajații favoriza politici agresive de investiție (de exemplu, Leeson avea un salariu de 50.000 de lire/an și spera la un bonus de nouă ori mai mare, bazat pe tranzacțiile derulate).

Exemplul 2

■ **Société Générale**

Una dintre cele mai mari bănci din Franța și acționar majoritar al Băncii Române pentru Dezvoltare, cu tradiție îndelungată în activitatea financiară (a fost fondată în 1864), avea să fie strașnic zguduită în anul 2008 de un scandal după ce a raportat o pierdere uriașă (de 7,2 miliarde de dolari) provenită din tranzacții cu instrumente financiare derivate. Nu numai că a fost cea mai mare pierdere raportată vreodată până la acel moment în lumea financiară, dar imediat agenția de rating Moody's a redus ratingul băncii de la Aa1/B la Aa2/B-.

Ce s-a întâmplat? Un trader începător (junior), Jérôme Kerviel, a decis să nu își respecte responsabilitățile funcției (de a specula diferențele dintre cursurile la vedere și cele la termen pentru instrumentele de capital) și să parieze pe indicele european Stock Index folosind contracte futures. Din păcate, alegerea lui a dus la pierderea menționată, care nu s-a mai recuperat niciodată.

Și în acest caz tot eșecul sistemului de control intern (faptul că salariatul a angajat banca într-o activitate pentru care nu avea autorizare, că nu a fost supravegheat adecvat, că a putut genera o pierdere așa de mare fără să îl oprească nimeni între timp, că nu existau limite de competență, că timp de doi ani, cât a desfășurat operațiunile respective, nu a sesizat nimeni depășirea atribuțiilor sale, că nu existau activități de monitorizare, că lipsea comunicarea între departamente și nu se făceau reconcilieri) a fost principalul motiv pentru pierderea raportată de banca Société Générale. Suplimentar, Kerviel a reușit să își ascundă tranzacțiile și pierderile profitând de competențele în IT pe care le avea (se pare că a făcut înregistrări fictive), ceea ce arată deficiențe majore și la sistemele informatice ale băncii.

Toate aceste minusuri au venit pe fondul unei culturi care se pare că încuraja comportamentele lipsite de etică. Traderul a declarat că și în trecut se întâmplase să își depășească atribuțiile, dar atâta timp cât rezultatele erau pozitive nimeni nu a zis nimic, ba, mai mult, a fost încurajat să continue.

Salariații și managerii primeau bonusuri importante calculate ca procent din profiturile generate pentru bancă, fiind astfel direct interesați să investească în tranzacții riscante, dar cu potențial mare de câștig.

Ulterior, Société Générale a declarat că a remediat deficiențele constatate.

4. Informarea și comunicarea

Un sistem informațional implică atât infrastructură (hardware), cât și componente software (aplicații), resurse umane, proceduri și date. În prezent, majoritatea sistemelor informaționale utilizează în mod extensiv tehnologia informației. Ele sunt responsabile cu prelucrarea și raportarea nu numai a datelor produse pe plan intern, ci și a celor provenite din exteriorul entității, rapoartele generate de acesta cuprinzând informații operaționale, financiare, nefinanciare și de conformitate pe care cei din conducere le folosesc în administrarea zilnică a afacerii.

Sistemul informațional joacă un rol semnificativ în administrarea societății, deoarece, în funcție de calitatea informațiilor generate, conducerea poate lua decizii adecvate privind gestionarea resurselor și a activității companiei, iar situațiile financiare pot reflecta cu fidelitate rezultatele obținute de aceasta.

Pentru a fi utile în luarea unei decizii, informațiile trebuie să aibă anumite caracteristici, adică trebuie să fie:

- relevante (utile într-o anumită situație);
- clare (ușor de înțeles de către persoanele care sunt familiarizate cu noțiunile respective);
- complete;
- corecte;
- credibile (imparțiale și provenite din surse de încredere);
- concise și adaptate nivelului de decizie care le folosește (spre exemplu, într-un fel va arăta raportul destinat CEO-ului companiei și altfel cel adresat directorului de vânzări pentru o anumită regiune);
- furnizate în timp util;
- comunicate persoanei potrivite și prin canalele corespunzătoare.

De asemenea, informațiile trebuie să aibă un raport cost-beneficii subunitar (adică beneficiile să fie superioare costurilor asociate cu obținerea lor).

Tot ca parte a componentei de informare și comunicare a controlului intern, acesta trebuie documentat. Gradul de complexitate al documentării (care poate avea diferite forme, cum ar fi cea narativă, cea bazată pe grafice sau scheme etc.) variază în funcție de complexitatea sistemului de control intern.

Comunicarea presupune înțelegerea rolurilor și responsabilităților individuale aferente atât controlului intern, cât și activităților derulate în general de entitate. Comunicarea este un proces care trebuie să se desfășoare în toate direcțiile (de sus în jos, respectiv de la conducere către salariați, dar și de jos în sus, adică informația care trebuie să ajungă la conducere, pe același palier (orizontal) și în exteriorul societății) și se poate face electronic, verbal sau prin intermediul acțiunilor conducerii. Conducerea trebuie să comunice valorile etice ale companiei, modul de comportare, importanța controlului intern, responsabilitățile și autorizările specifice, precum și toleranța față de risc proprie entității.

Potrivit ISA 315, sistemul informațional relevant pentru obiectivele de raportare financiară include sistemul de raportare financiară și înglobează metode care:

- identifică și înregistrează toate tranzacțiile valabile;
- descriu la timp tranzacțiile suficient de detaliat pentru a da posibilitatea clasificării lor adecvate pentru raportarea financiară;
- măsoară valoarea tranzacțiilor într-o manieră care permite înregistrarea valorii lor monetare corespunzătoare în situațiile financiare;
- determină perioada de timp în care au avut loc tranzacțiile pentru a da posibilitatea înregistrării lor în perioada contabilă adecvată;
- prezintă corespunzător tranzacțiile și informațiile aferente în situațiile financiare.

Comunicarea relevantă pentru raportarea financiară include, de regulă, manuale de politici contabile și proceduri și altele similare.

5. Monitorizarea controalelor

Conducerea este responsabilă și cu monitorizarea controlului intern, activitate care are ca scop principal asigurarea că toate controalele implementate continuă să funcționeze eficient în timp. Monitorizarea controalelor presupune evaluarea gradului în care acestea funcționează în modul în care au fost proiectate să funcționeze și a măsurii în care sunt modificate, dacă apar schimbări ale condițiilor. Cu alte cuvinte, prin monitorizarea controlului intern conducerea entității urmărește ca obiectivele generale ale acestuia să fie atinse.

Monitorizarea trebuie să includă politici și proceduri care să asigure soluționarea adecvată și promptă a constatărilor. Degeaba sunt identificate carențe ale controalelor interne dacă în urma acestei informații nu se iau măsuri operative. Mai mult, identificarea unei deficiențe semnificative și necorectarea ei imediată poate avea un efect mai defavorabil decât lipsa informației privind deficiența.

Concret, cei din conducere trebuie:

- să evalueze prompt constatările activității de monitorizare (fie că este vorba despre deficiențe, recomandări de îmbunătățire sau chiar bune practici care pot fi diseminate în continuare). Evaluarea poate să se refere la semnificația și iminența unui eventual răspuns necesar;
- să ia măsurile care se impun ca răspuns la constatările și recomandările menționate la pasul anterior. Măsurile depind, așa cum am spus, de semnificația și iminența unui eventual răspuns necesar;
- să finalizeze în intervale de timp stabilite toate măsurile de corectare sau de soluționare a aspectelor care le-au fost aduse în atenție.

Procesul de soluționare începe în momentul în care rezultatele monitorizării sunt raportate conducerii și este finalizat atunci când fie s-au luat măsuri care corectează deficiențele identificate sau aduc îmbunătățiri aspectelor sesizate, fie se concluzionează că respectivele constatări sau recomandări nu necesită măsuri manageriale (în sensul că riscul identificat privind eventualele deficiențe este mai mic decât cel tolerat de entitate).

Monitorizarea se poate realiza prin activități de monitorizare continuă, printr-o evaluare separată sau printr-o combinare a acestor două metode. Cea dintâi este considerată mai eficientă decât evaluările separate, care au loc după producerea faptului.

Monitorizarea continuă include activități de conducere și supervizare regulate, continue, care trebuie să acopere fiecare componentă a controlului intern și să fie încorporate în activitățile normale, recurente. Avantajul metodei constă în aceea că poate identifica în timp real eventualele deficiențe ale controlului intern.

Activitățile de monitorizare pot folosi informații din surse interne (spre exemplu, rapoartele primite în legătură cu funcționarea controlului intern) sau externe (reglementatorii, cum ar fi în România Autoritatea de Supraveghere Financiară (ASF), BNR sau alte instituții, auditorii externi ori diverși terți).

Evaluările separate presupun monitorizarea cu caracter ocazional pe care o pot cere/efectua cei din conducere. Avantajul constă în aceea că ele se concentrează direct asupra eficienței anumitor controale la un moment dat. Frecvența și acoperirea acestora depind de riscurile evaluate specifice acelor controale interne, precum și de eficiența procedurilor de monitorizare continuă.

Auditorilor interni sau altor angajați cu atribuții în controlul intern li se poate cere să efectueze misiuni speciale de monitorizare, în cadrul cărora ei evaluează eficacitatea controlului intern, raportează cu privire la punctele forte și deficiențele acestuia și fac recomandări pentru îmbunătățirea lui. Constatările trebuie raportate nivelului corespunzător de conducere.

Bibliografie

1. Deloitte & Touche LLP (2012), *Risk Assessment in Practice*, ghid pregătit pentru COSO.
2. https://www.coso.org/Pages/default.aspx
3. https://www.coso.org/Pages/erm-integratedframework.aspx

Acest articol este preluat din lucrarea *Guvernanța corporativă, managementul riscurilor și controlul intern*, autor Mirela Păunescu, apărută la Editura CECCAR în anul 2019.