GUID 5101

Ghidurile (GUIDs) sunt emise de către INTOSAI, Organizația Internațională a Instituțiilor Supreme de Audit. Pentru mai multe informații accesați *www.issai.org*

INTOSAI

Proiect pentru expunere

Ghid privind Auditul Securității Sistemelor Informatice

EXPOSURE DRAFT

noiembrie 2018

I N T O S A I

EXPOSURE DRAFT

Secretariatul General al INTOSAI
RECHNUNGSHOF
(Curtea de Conturi a Austriei)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at;
WORLD WIDE WEB: http://www.intosai.org

Cuprins

1. Introducere

1.1 GUID 5101 asigură cadrul pentru efectuarea Auditului Securității Sistemelor Informatice conform IFPP. Cadrul prezentat în acest document GUID este în concordanță cu Principiile Fundamentale ale Auditului Sectorului Public (ISSAI 100), Principiile Auditului Performanței (ISSAI 300), Principiile Auditului de Conformitate (ISSAI 400) și Ghidul de Audit al Sistemelor Informatice (GUID 5100).

1.2 GUID 5101 prezintă concepte și îndrumări privind Auditul Securității Sistemelor Informatice, inclusiv Securitatea Cibernetică, ce sunt detaliate suplimentar, în beneficiul practicienilor din cadrul Instituțiilor Supreme de Audit, în Manualul WGITA-IDI privind Auditul IT.

1.3 Multe dintre entitățile auditate din sectorul public prelucrează și lucrează cu date confidențiale legate de stat, precum și date sensibile legate de cetățeni – date demografice, biometrice, bancare, bursiere, istoricul medical, nivelul de studii, istoricul activității profesionale, date fiscale, situația antecedentelor judiciare, cazierul judiciar etc., fiind necesar ca acestea să poată fi transmise și stocate în siguranță în interesul public. Deținătorii unor astfel de sisteme informatice trebuie să se asigure că informația este disponibilă atunci când este solicitată și utilizată numai de către personalul autorizat în scopurile hotărâte. Ca urmare, devine imperativă dezvoltarea de către un SAI a capacității adecvate de efectuare a examinării temeinice a auditurilor privind Securitatea Sistemelor Informatice în sectorul public.

2. Obiectivele prezentului GUID

2.1 ISSAI 100, 200, 300 și 400 stabilesc principiile de bază ale auditării în ceea ce privește Auditul de Conformitate, Auditul Performanței și Auditul Financiar. Aceste standarde ISSAI se referă la principii generale, proceduri, standarde și așteptări din partea unui auditor. În timp ce GUID 5100 prevede îndrumări specifice temei Auditului Sistemelor Informatice, inclusiv domeniului Securității Sistemelor Informatice, obiectivul prezentului document GUID este de a oferi auditorilor îndrumări procedurale suplimentare cu privire la realizarea activităților de audit în domenii specifice Securității Sistemelor Informatice.

2.2 Conținutul prezentului GUID se poate aplica de către auditori în următoarele etape ale procesului de auditare: Planificare, Execuție, Raportare și Verificare a modului de implementare a recomandărilor (follow-up)[1].

3. Definiții

3.1 Securitatea informațiilor dintr-un sistem informatic poate fi definită drept un set de controale privitoare la politici, structuri și procese al căror scop este de a împiedica accesul, folosirea, dezvăluirea, perturbarea, modificarea, examinarea, înregistrarea sau distrugerea neautorizate ale informațiilor stocate într-un sistem informatic. Ca urmare, pentru un sistem bazat pe IT, Managementul Securității Informației constă în acele audituri IT al căror scop este de a asigura confidențialitatea, integritatea și disponibilitatea datelor în cadrul sistemului informatic.

3.2 Managementul Securității Cibernetice se poate defini ca un set de audituri referitoare la politici, structuri și procese al căror scop este de a proteja activele digitale[2]- hardware și informații - împotriva deteriorării, a accesării sau modificării neautorizate, sau a exploatării[3]. Atacuri externe asupra unor asemenea sisteme informatice – care pot fi găzduite pe sau

[1] ISSAI 100

[2] Cyber Security Fundamentals Study Guide (în traducere *Ghidul de Studiu al Elementelor Fundamentale ale Securității Cibernetice*) 2015 - ISACA

[3] Glosar de termeni, US-CERT

EXPOSURE DRAFT

conectate la Internet – pot fi inițiate de către persoane rău-intenționate, entități finanțate de stat, sau de către grupuri care au un anumit interes în legătură cu datele sau au ca scop perturbarea operațiunilor comerciale. Dat fiind că multe sisteme informatice din sectorul public colectează și stochează informații sensibile despre cetățeni, este imperios necesar ca astfel de sisteme informatice să adopte măsuri adecvate de Securitate Cibernetică. Astfel de măsuri de Securitate cibernetică pot include funcții cheie[4] privitoare la managementul incidentelor, precum:

- Identificarea nivelurilor de risc aplicabile sistemelor, activelor, datelor și capacităților
- Protejarea infrastructurii și a serviciilor esențiale împotriva impactului potențialelor amenințări
- Detectarea apariției unor evenimente legate de securitate
- Inițierea răspunsului ulterior descoperirii unor evenimente legate de securitate
- Recuperarea la timp a capacităților și serviciilor compromise

3.3 Auditul de Securitate, inclusiv Securitate Cibernetică, al Sistemelor Informatice poate, așadar, fi definit drept o misiune de audit specifică subiectului analizat, care implică examinarea controalelor de IT care fac parte din Managementul Securității Informației, pentru a identifica situații de abateri de la criterii, care, la rândul lor, au fost identificate pe baza tipului de misiune de audit. Spre exemplu, auditorul intenționează să se asigure

- ca parte dintr-un Audit Financiar, că sistemul bazat pe IT este îndeajuns de sigur pentru a asigura adeziunea la cadrul acceptat de reglementare și raportare financiară.
- ca parte dintr-un Audit al Performanței, că sistemul bazat pe IT este îndeajuns de sigur pentru a da posibilitatea intervențiilor, programelor și instituțiilor să funcționeze în conformitate cu principiile economicității, eficienței și eficacității.
- ca parte dintr-un Audit de Conformitate, că sistemul bazat pe IT este îndeajuns de sigur pentru a asigura conformitatea cu legile / reglementările aplicabile.

4. Arie de cuprindere

4.1 Prezentul document poate fi folosit de către auditori pentru a efectua Audituri Financiare/ ale Performanței/ de Conformitate cu privire la subiectul specific al Securității Sistemelor Informatice.

4.2 Aceste linii directoare oferă îndrumări suplimentare cu privire la modul în care Auditul de Securitate al Sistemelor Informatice poate fi abordat prin utilizarea auditului financiar / al performanței / de conformitate și nu conține alte cerințe pentru efectuarea auditului.

[4] Adaptat după cadrele de Securitate Cibernetică ale Institutului Național de Standarde și tehnologie (NIST) și Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

5. Planificarea auditului securității sistemelor informatice

5.1 Instituțiile Supreme de Audit pot adopta o planificare a auditului bazată pe risc pentru examinarea securității Sistemelor Informatice, în concordanță cu procesul descris pentru Auditul Financiar (ISSAI 200), Auditul Performanței (ISSAI 300), Auditul de Conformitate (ISSAI 400) și Auditul Sistemelor Informatice (GUID 5100).

5.2 Scopul unei misiuni de audit privind securitatea sistemelor informatice este de a examina controalele IT adoptate de către entitatea auditată în sistemele sale informatice pentru a asigura confidențialitatea, integritatea și disponibilitatea informației.

5.3 În cadrul obiectivului mai amplu menționat anterior, aria de cuprindere a obiectivelor și sub-obiectivelor unei misiuni de audit privind Securitatea Sistemelor Informatice poate aparține oricăruia dintre sau tuturor domeniilor[5] entității auditate. Anexa prezentelor îndrumări conține o listă ilustrativă de obiective de audit și de sub-audit legate de aceste domenii -

- Politica Organizațională privind Securitatea Informației
- Structura Guvernanței Organizaționale privind Securitatea Informației
- Securitatea Activelor Informaționale
- Securitatea în procesele de Dezvoltare, Achiziție și Întreținere a Sistemelor Informatice
- Securitatea Operațiunilor IT
- Securitatea Mediului Fizic
- Aspecte de securitate ce țin de Resursele Umane care operează cu Sistemele Informatice
- Securitatea Managementului Comunicării
- Aspecte de securitate legate de cerințele statutare de conformitate
- Aspecte de securitate în procesele de management al continuității activității și al recuperării în caz de dezastru
- Aspecte de securitate în controalele de aplicație în cadrul sistemelor informatice individuale[6]

5.4 Auditorii pot lua în considerare adaptări după cadrele de securitate a informațiilor existente[7], pentru analiza potențialelor obiective de audit. În Anexa A se regăsește o listă indicativă, și nu exhaustivă, de obiective și sub-obiective pentru fiecare dintre domeniile menționate mai sus.

5.5 SAI-urile pot observa faptul că securitatea informațiilor este o funcție orizontală, care are impact asupra tuturor celorlalte domenii, menționate mai sus, ale unei entități în cadrul căreia IT-ul joacă un rol esențial. Este posibil să fie necesar ca SAI-urile să ia în considerare diverse tendințe tehnologice[8] cum ar fi:

- Platformele și instrumentele folosite
- Conectivitatea rețelei (interne, ale terților părți, publice)
- Nivelul de complexitate IT
- Asistență operațională pentru securitate
- Capacitățile și comunitatea utilizatorilor

[5] Adaptat după ISO/IEC 27001

[6] Controalele de Aplicație sunt proceduri manuale sau automate încorporate într-un sistem bazat pe IT, care sunt legate de validarea datelor de intrare, procesarea corectă a datelor, livrarea datelor de ieșire și controale legate de integritatea master data.

[7] Anexa *Reference control objectives and controls* din ISO/IEC 27001; Partea VI din "Programul de Audit al Managementului Securității Informației" al ISACA

[8] Ghidul de Studiu al Elementelor Fundamentale ale Securității Cibernetice 2015 - ISACA

EXPOSURE DRAFT

- Instrumente de securitate noi sau în curs de dezvoltare

care pot afecta Securitatea informațiilor entității auditate.

6. Efectuarea auditului securității sistemelor informatice

6.1 Auditorii pot adopta procesele descrise pentru Auditul Financiar (ISSAI 200), Auditul Performanței (ISSAI 300), Auditul de Conformitate (ISSAI 400) și Auditul Sistemelor Informatice (GUID 5100) , atunci când efectuează auditul securității sistemelor informatice.

6.2 Instituțiile Supreme de Audit pot efectua evaluarea controalelor IT adoptate de către entitatea auditată pentru Securitatea Sistemelor Informatice, în scopul de a verifica caracterul demn de încredere și suficiența acestora, prin folosirea tehnicilor descrise în GUID 5100. Aria de cuprindere a evaluării controalelor IT pentru securitate poate include următoarele verificări:

- dacă Politica Organizațională de Securitatea Informației a fost definită, adoptată și comunicată
- dacă structura Guvernanței Organizaționale a Securității Informației a fost stabilită și este funcțională
- dacă s-a realizat inventarul periodic al activelor IT și dacă au fost identificate cerințele de securitate corespunzătoare fiecărui tip de activ
- dacă au fost definite, adoptate și comunicate procesele de Securitate pentru dezvoltarea, achiziția și întreținerea Sistemelor Informatice
- dacă au fost definite, adoptate și comunicate procesele privind securitatea operațiunilor (internalizare, externalizare, contracte de prestări servicii)
- dacă s-au luat măsuri menite să asigure securitatea fizică și să garanteze condițiile fizice de lucru plănuite.
- dacă s-au adoptat măsuri de securitate privind selectarea candidaților înainte de recrutarea, instruirea și sensibilizarea resurselor umane cu privire la aspectele legate de securitatea informației, definirea diferitelor funcții și separarea funcțiilor, precum și măsuri de securitate care să fie puse în aplicare odată cu încetarea relațiilor contractuale
- dacă s-au adoptat măsuri care să asigure confidențialitatea, integritatea și disponibilitatea diverselor modalități și canale de comunicare
- dacă s-au adoptat măsuri pentru securitatea cerințelor statutare de conformitate
- dacă s-au adoptat măsuri privind Securitatea Continuității Activității și procesele de Management al Recuperării în caz de Dezastru
- dacă, controalele de aplicație privitoare la Securitate, din cadrul fiecărui sistem informatic, sunt adecvate și demne de încredere. O astfel de evaluare poate include identificarea unor componente semnificative ale aplicației, identificarea gradului de importanță al aplicației pentru entitate, analizarea documentației disponibile, intervievarea personalului, înțelegerea riscurilor de securitate ale controlului de aplicație precum și impactul acestora asupra entității, și elaborarea de teste care să examineze adecvarea și caracterul demn de încredere al unor astfel de controale de aplicație.

6.3 Evaluarea controalelor IT legate de Securitatea Informației poate cuprinde politicile, procesele, personalul și sistemele entității auditate, în concordanță cu obiectivele Auditului. Această evaluare comprehensivă poate fi adaptată de către SAI-uri pe baza cadrelor de securitate a informațiilor existente[9] sau prin dezvoltarea de noi cadre adecvate. În Anexa A se

[9]Anexa *Reference control objectives and controls* din ISO/IEC 27001:2013; Partea VI din Programul de Audit al Managementului Securității Informației" al ISACA

regăsește o listă indicativă, și nu exhaustivă, de evaluări grupate pe sub-obiective pentru fiecare dintre domeniile menționate mai sus.

7. Raportarea în Auditul Securității Sistemelor Informatice

7.1 Dat fiind că o misiune de audit privind Securitatea Sistemelor Informatice se bazează pe unul sau mai multe dintre tipurile principale de audit, auditorii pot considera cerințele de raportare pentru astfel de misiuni de audit ca fiind echivalente cu cele pentru Auditul Financiar (ISSAI 200), Auditul Performanței (ISSAI 300) și Auditul de Conformitate (ISSAI 400). Îndrumările pentru raportare ar fi în mare parte asemănătoare cerințelor descrise în GUID 5100.

8. Verificarea modului de implementare a recomandărilor (follow-up)

8.1 Dat fiind că o misiune de audit privind Securitatea Sistemelor Informatice se bazează pe unul sau mai multe dintre tipurile principale de audit, auditorii pot considera cerințele de verificare a modului de implementare a recomandărilor pentru astfel de misiuni de audit ca fiind echivalente cu cele pentru Auditul Financiar (ISSAI 200), Auditul Performanței (ISSAI 300) și Auditul de Conformitate (ISSAI 400). Îndrumările pentru follow-up ar fi, în mare, similare cerințelor descrise în GUID 5100.

Anexa A - Matricea Indicativă de Audit

Prezenta Anexă conține obiective generice privitoare la aspectul specific al Auditului de Securitate a Informațiilor sub forma unor îndrumări, și are caracter doar indicativ și nu exhaustiv. Pentru liste de verificare a auditului mai detaliate și matrici de audit pentru fiecare dintre domeniile IT și aspectele legate de securitate, Instituțiile Supreme de Audit pot consulta Manualul WGITA-IDI privind auditul IT.

Nr. SI	Domeniu în Securitatea Informației	Obiectiv	Sub-obiectiv	Evaluarea ce se va efectua
1	Politica organizațională de Securitate a Informației	Dacă o astfel de politică este definită, adoptată și comunicată.	NA	Se verifică claritatea din documentație cu privire la definiții și obiective, se verifică adoptarea de către Autoritatea Competentă, și se verifică publicarea / comunicarea / înștiințarea tuturor părților interesate.
2	Structură de guvernanță organizațională a Securității Informației	Dacă este stabilită și funcțională o astfel de structură.	Dacă o astfel de structură de guvernanță este în mod clar răspunzătoare de toate chestiunile ce țin de securitatea informației.	Se verifică claritatea documentației în privința definițiilor, a constituirii, a alcătuirii și a mandatului.
			Dacă au fost definiți termenii de personal - ca parte a acestei structuri de guvernanță -, roluri individuale și mecanisme de raportare.	Se verifică claritatea documentației în privința personalului individual, a rolurilor și responsabilităților pentru fiecare categorie de personal și a ierarhiei de raportare a problemelor.
			Dacă structura de guvernanță analizează periodic problemele legate de Securitatea Informației și dacă se aplică măsurile recomandate în privința chestiunilor identificate.	Se verifică documentația pentru a analiza frecvența și ordinea de zi a întâlnirilor structurii de guvernanță, lista chestiunilor identificate ca necesitând anumite măsuri și măsurile întreprinse în mod real.
3	Gestionarea activelor	Dacă s-a efectuat în mod periodic inventarul	Dacă s-a efectuat în mod periodic inventarul tuturor activelor IT ale organizației.	Se verifică modulele de sistem în managementul materialelor, rapoartele

		activelor IT și dacă s-au identificat cerințele de securitate pentru fiecare tip de active.		de inspecție și alte documentații legate de inventarul activelor IT. Se examinează prin eșantionare pentru a se stabili dacă lista de active este completă și corectă, și dacă aceasta este actualizată.
			Dacă activele IT sunt clasificate pe criteriul gradului de importanță în raport cu cerințele organizaționale.	Se verifică modulele de sistem / documentația pentru a vedea dacă activele IT sunt clasificate pe baza costurilor de înlocuire, a costurilor ce ar fi suportate de către organizație în cazul nefuncționării sau a altor parametri.
			Dacă au fost stabilite cerințele de securitate pentru fiecare tip de activ.	Se verifică modulele de sistem/documentația pentru a vedea dacă se identifică la intervale regulate cerințele de creștere a capacității activelor pentru fiecare tip de active, listele de active, pentru fiecare tip de active, care necesită înlocuirea deoarece sunt învechite, listele de active, pentru fiecare tip de active, care urmează să fie scoase din uz, deoarece nu mai prezintă siguranță în fața noilor amenințări externe.
4.	Dezvoltarea, achiziția și întreținerea sistemelor informatice	Dacă aspectele legate de securitate pentru fiecare dintre aceste procese au fost definite, adoptate și comunicate.	Dacă criteriile de dezvoltare vs. decizia de achiziționare de sisteme informatice includ criterii legate de asigurarea securității informației.	Se verifică dacă analiza cost-beneficiu efectuată cu scopul de a permite luarea unei decizii cu privire la dezvoltare versus achiziție a luat în considerare costul indirect presupus de asigurarea securității informațiilor împărtășite vânzătorului produselor

				necesare dezvoltării sau furnizorului în cazul achiziției, întrucât în fiecare situație, ambii vânzători ar avea nevoie să poată accesa, cel puțin, date istorice pentru a efectua testele premergătoare acceptării de către utilizator și alte teste.
			Dacă sistemele informatice dezvoltate prin intermediul vânzătorilor / achiziționate de la furnizori au fost verificate pentru a împiedica atacurile prin caracteristici ascunse.	Se verifică dacă entitatea auditată a solicitat examinarea codului și a modulelor sistemului informatic dezvoltat / achiziționat de către resurse interne sau externe abilitate pentru a se asigura că nu există caracteristici ascunse care ar putea compromite confidențialitatea, integritatea și disponibilitatea datelor.
			Dacă furnizorilor de servicii de mentenanță li se oferă acces doar la acele module ale sistemului informatic și doar la acele date care sunt necesare îndeplinirii funcției de mentenanță.	Se verifică dacă s-au implementat controale de acces în sistemul informatic pentru a împiedica furnizorul serviciilor de mentenanță să provoace modificări neautorizate ale acestuia, care ar putea compromite confidențialitatea, integritatea și disponibilitatea datelor.
			Dacă, cerințele de securitate ale organizației sunt incluse în contractele / acordurile privind calitatea serviciilor încheiate cu furnizorii acestor procese.	Se examinează contractele/acordurile privind calitatea serviciilor pentru a se verifica includerea clauzelor de confidențialitate, de neconcurență, de nemodificare în lipsa autorizării, de

EXPOSURE DRAFT

				netransmisibilitate, precum și alte prevederi standard legate de asigurarea confidențialității, integrității și disponibilității datelor.
5.	Operațiuni IT	Dacă securitatea operațiunilor IT a fost definită, adoptată și comunicată.	NA	Se examinează contractele/acordurile privind calitatea serviciilor încheiate cu părți către care se externalizează operațiuni IT, pentru a se verifica includerea clauzelor de confidențialitate, de non-concurență, de nemodificare în lipsa autorizării, de netransmisibilitate, precum și alte prevederi standard legate de asigurarea confidențialității, integrității și disponibilității datelor.
6	Mediul fizic	Dacă s-a asigurat securitatea mediului fizic al sistemului informatic.	Dacă accesul fizic la echipamentele hardware de stocare ale sistemului informatic este permis numai personalului autorizat.	Se verifică existența barierelor fizice (porți la exterior, uși la interior, paznici) care să solicite identificarea personalului și să permită accesul la echipamentele hardware de stocare, cum ar fi serverele, doar personalului autorizat.
			Dacă accesul fizic la sediile clientului din care, în mod logic, se pot accesa datele stocate, este permis doar personalului autorizat.	Se verifică existența barierelor fizice (porți la exterior, uși la interior, paznici) care să solicite identificarea personalului și să permită accesul la echipamentele hardware de stocare, cum ar fi serverele, doar personalului autorizat.

			Dacă mediul fizic de depozitare a echipamentelor hardware ale sistemului informatic poate păstra condițiile fizice dorite, referitoare la temperatură, umiditate, aerisire, umezeală și absența animalelor dăunătoare.	Se verifică dacă proiectul, materialele și tiparul construcției sunt adecvate pentru a asigura un mediu fără umezeală și animale dăunătoare. Se verifică dacă echipamentele sistemului de climatizare (HVAC [10]) sunt instalate, funcționează corect și revizia acestora se efectuează periodic astfel încât să se asigure păstrarea temperaturii, umidității și curățeniei dorite a mediului fizic.
			Dacă s-a asigurat furnizarea neîntreruptă a energiei electrice precum și o sursă de curent de rezervă	Se verifică dacă sunt instalate atât sursa normală de alimentare cu energie electrică cât și cea de rezervă și dacă acestea sunt adecvate pentru a reduce riscul de întrerupere a alimentării cu energie electrică la un nivel acceptabil.
7	Resurse umane	Dacă s-au abordat aspectele de securitate legate de resursele umane implicate în utilizarea sistemelor informatice.	Dacă resursele umane au fost instruite în mod adecvat cu privire la importanța păstrării confidențialității, integrității și disponibilității datelor.	Se verifică dacă s-a efectuat instruirea periodică cu privire la aspecte cum ar fi crearea unei culturi a conștientizării securității, importanța nedezvăluirii și netransmisibilității informațiilor către personal neautorizat în vederea păstrării confidențialității, importanța modificării datelor doar ulterior obținerii autorizațiilor necesare în vederea păstrării integrității

[10] HVAC – Heating, Ventilation, Air-Conditioning (*Încălzire, Ventilare, Aer Condiționat*)

				datelor și nedivulgarea parolelor și a altor date de autentificare pentru a împiedica atacurile de blocare a serviciului ale unor utilizatori rău-intenționați.
			Dacă rolurile și privilegiile de acces ale fiecărui utilizator sunt clar definite.	Se verifică dacă au fost clar definite rolurile și responsabilitățile managementului, și anume Director Tehnologia Informației, Custode al Datelor, Proprietar de Sistem, Administrator de Securitate, Analist de Securitate.
			Dacă s-a implementat separarea funcțiilor pentru a se asigura principiul echilibrului instituțional.	Se verifică dacă există o separare clară a rolurilor pentru a preveni conflictele de interese, mai ales acelea care, laolaltă, pot crea ocazii pentru încălcarea confidențialității, a integrității și a disponibilității datelor.
8	Managementul comunicațiilor	Dacă s-au abordat aspectele de securitate legate de modurile și canalele de comunicare.	Dacă mesajele de comunicare sunt codificate.	Se verifică dacă, canalele de comunicare asigură codificarea tuturor mesajelor, pentru a împiedica intervenția terțelor părți și pierderea confidențialității.
			Dacă expeditorul poate renega mesajele de comunicare ulterior.	Se verifică dacă, canalele de comunicare au încorporată funcție de non-repudiere.
			Dacă a fost definită limita maximă a utilizatorilor concomitenți.	Se verifică dacă s-a definit și este funcțională limita maximă a utilizatorilor concomitenți, pentru a împiedica accesarea sistemului informatic de către utilizatori suplimentari, asigurând în același timp

				necompromiterea disponibilității datelor în orice moment pentru utilizatori până la limita definită.
9	Conformitatea statutară	Dacă s-au respectat cerințele statutare legate de aspectele ce țin de securitatea informațiilor.	Dacă cerințele statutare de conformitate au fost comunicate intern de către entitatea auditată.	Se verifică documentația cu privire la comunicarea internă pe acest subiect către toate părțile interesate.
			Dacă au fost informate centrele interne de responsabilitate însărcinate cu asigurarea conformității statutare.	Se verifică documentația cu privire la comunicarea internă pe acest subiect către toate părțile interesate.
			Dacă cerințele statutare de conformitate ce țin de securitatea informațiilor au fost puse în corespondență cu logica de programare / controalele interne ale sistemelor informatice.	Se verifică dacă fiecare cerință statutară a fost pusă în mod adecvat în corespondență cu logica de programare / controalele interne din cadrul sistemelor informatice utilizate de către entitatea auditată.
			Dacă situația conformității cu cerințele statutare se raportează autorităților adecvate conform intervalelor prestabilite.	Se verifică dacă rapoartele privind situația conformității/excepțiilor se depun la autoritățile adecvate prestabilite de către entitatea auditată.
10	Managementul continuității activității și recuperării în caz de dezastru	Dacă s-au abordat aspectele de securitate legate de aceste procese.	Dacă și amplasamentul de rezervă, aflat în afara sediului principal, are aranjamente ce țin de securitatea fizică asemănătoare celor din sediul principal.	Se verifică dacă aranjamentele adecvate au fost reproduse în amplasamentul aflat în afara sediului principal.
			Dacă a fost definită periodicitatea creării copiilor de siguranță în funcție de riscul de securitate.	Se verifică dacă periodicitatea creării copiilor de siguranță este proporțională cu funcția și gradul de importanță ale sistemului informatic

				pentru organizație. Pentru sistemele de informații care se bazează pe colectarea, stocarea și procesarea datelor în timp real, păstrarea unui server oglindă ar putea fi mai potrivită decât efectuarea zilnică a unor copii de rezervă, chiar dacă acest tip de back-up este costisitor.
			Dacă amplasamentul de rezervă se află în condiții rezonabile de siguranță împotriva catastrofelor naturale, cum ar fi cutremurele sau tsunami.	Se verifică dacă amplasamentul de rezervă se află într-o zonă cu risc seismic relativ scăzut și unde riscul unor asemenea catastrofe naturale este la un nivel minim acceptabil.
			Dacă s-au efectuat exerciții de simulare a utilizării datelor stocate în amplasamentul de rezervă.	Se verifică dacă datele din amplasamentul de rezervă aflat în afara sediului principal au fost testate pentru a vedea dacă pot fi folosite cel puțin într-un mediu de testare, astfel încât toți utilizatorii și personalul să fie familiarizați cu procedeele ce trebuie urmate pentru a asigura continuitatea activității.
11	Controale de aplicație	Dacă s-au adoptat controale de aplicație adecvate în sistemul informatic.	Dacă s-au definit în mod clar permisiunile și privilegiile de acces.	Se verifică datele primare (master data) pentru personalul căruia i s-a permis accesarea diverselor tipuri de date și se analizează abaterile de la definiții.
			Dacă s-a realizat în mod corect autentificarea personalului înainte de a-i furniza acces la vizualizarea datelor.	Se verifică dacă personalul poate accesa informațiile, conform permisiunilor, doar ulterior introducerii datelor de autentificare corecte, cum ar fi parole sau date biometrice, și

				se analizează abaterile de la aceasta prin verificarea datelor tranzacționale.
			Dacă modificarea datelor a fost realizată numai de către personalul autorizat.	Se verifică din conectările utilizatorilor, dacă modificările datelor au fost realizate numai de către acei membri ai personalului care aveau permisiunea de a efectua respectivele modificări.
			Dacă personalul are permisiunea de a accesa sau modifica date din oricare dintre sediile clienților sau în orice moment.	Se verifică din conectările utilizatorilor și marcajul temporal, dacă vreunul dintre membrii personalului, inclusiv cei autorizați, a accesat / modificat date aflându-se în alte locuri și nu la birou sau acasă și în afara orelor de lucru definite.
			Dacă personalul are permisiunea de a transmite / stoca o rezervă personală a datelor.	Se verifică din conectările utilizatorilor și marcajul temporal, dacă vreunul dintre membrii personalului, inclusiv cei autorizați, a accesat / modificat date transmițându-le ulterior prin orice metodă de comunicare în afara serviciului sau efectuând ulterior copii de rezervă ale datelor.