Anexa nr. 5

Clasificarea pe categorii de riscuri a riscurilor TIC care pot genera pierderi cu un grad ridicat de severitate și descrierea lor

Categorii de riscuri TIC	Riscuri TIC, listă non-exhaustivă	Descrierea riscului
Riscuri de disponibilitate și continuitate TIC	Gestionarea unor capacități insuficiente	O lipsă de resurse (hardware, software, personal, furnizori de servicii) poate duce la imposibilitatea de a dimensiona în mod corespunzător serviciul pentru îndeplinirea nevoilor de afaceri, la întreruperi de sistem, la degradarea serviciului și/sau la erori operaționale.
	Defecțiuni ale sistemelor TIC	Pierderea disponibilității din cauza defecțiunilor la componenta hardware a TIC.
		Pierderea disponibilității din cauza erorilor la componenta software a TIC și a erorilor de tip bug.
	O planificare inadecvată a continuității și a recuperării TIC ca urmare a dezastrelor	Eșecul soluțiilor TIC de disponibilitate și/sau continuitate planificate și/sau nerecuperarea acestora ca urmare a dezastrelor (de exemplu, centru de date de recuperare) atunci când sunt activate ca răspuns la producerea unui incident.
	Atacuri cibernetice perturbatoare și distructive	Atacurile prevăzute pentru diferite scopuri (de exemplu, activism, șantaj), care determină supraîncărcarea sistemelor și a rețelei, împiedicând accesarea serviciilor informaționale online de către utilizatorii legitimi ai acestora.
Riscuri de securitate TIC	Atacuri cibernetice și alte atacuri externe bazate pe TIC	Atacurile lansate de pe Internet sau din rețele din exterior în diferite scopuri (de exemplu, fraudă, spionaj, activism/sabotaj, terorism cibernetic) printr-o varietate de tehnici (de exemplu, inginerie socială, încercări de pătrundere forțată prin exploatarea vulnerabilităților, transmiterea de software dăunător) care duc la preluarea controlului asupra sistemelor TIC interne.
		Executarea de tranzacții de plăți frauduloase de către hackeri prin spargerea sau ocolirea sistemului de securitate al serviciilor bancare electronice și de plată

		și/sau prin atacarea și exploatarea vulnerabilităților de securitate din cadrul sistemelor de plată interne ale instituției de credit.
		Executarea de către hackeri a tranzacțiilor frauduloase cu valori mobiliare prin spargerea sau ocolirea sistemului de securitate al serviciilor bancare electronice care asigură și accesul la conturile de valori mobiliare ale clienților.
		Atacuri asupra conexiunilor de comunicare și a conversațiilor de orice fel sau a sistemelor TIC cu obiectivul de a colecta informații și/sau a comite fraude.
	Securitate TIC internă inadecvată	Obținerea accesului neautorizat la sisteme TIC critice din interiorul instituției de credit în diferite scopuri (de exemplu, fraudă, desfășurarea și ascunderea de tranzacții frauduloase, furtul de date, activism/sabotaj) printr-o varietate de tehnici (de exemplu, abuzul de și/sau sporirea privilegiilor, furtul de identitate, ingineria socială, exploatarea vulnerabilităților din sistemele TIC, transmiterea de software dăunător).
		Cazuri de manipulare TIC neautorizată din cauza procedurilor și practicilor de gestionare a accesului TIC necorespunzătoare.
		Amenințări la adresa securității din cauza lipsei de cunoștințe despre securitate, situații în care angajații nu înțeleg, neglijează sau nu respectă politicile și procedurile de securitate TIC.
		Stocarea sau transferul neautorizat de informații confidențiale în afara instituției de credit.
	Securitate TIC fizică inadecvată	Deturnarea sau furtul de active TIC prin accesul fizic, provocând daune, pierderea de active sau date sau materializarea altor amenințări.
		Deteriorarea intenționată sau accidentală a activelor TIC fizice din cauza terorismului, a accidentelor sau a utilizării eronate din partea angajaților instituției de credit și/sau a terților (furnizori, reparatori).
		Protejarea fizică insuficientă împotriva calamităților naturale, care duc la

		distrugerea parțială sau completă a sistemelor TIC/centrelor de date.
Riscuri de schimbare TIC	Proceduri de control inadecvate pentru schimbări aduse sistemului TIC sau dezvoltarea acestuia.	Incidente provocate de erori sau vulnerabilități nedepistate ca urmare a schimbărilor (de exemplu, efecte neprevăzute ale unei schimbări sau o schimbare gestionată necorespunzător din cauza lipsei testării sau a practicilor necorespunzătoare de gestionare a schimbărilor) aduse, spre exemplu, software-ului, sistemelor și datelor TIC.
	Arhitectura TIC inadecvată	O administrare defectuoasă a arhitecturii TIC la proiectarea, dezvoltarea și întreținerea sistemelor TIC (de exemplu, software, hardware, date) poate duce, în timp, la o administrare complexă, dificilă, costisitoare și la sisteme TIC rigide care nu mai sunt suficient armonizate cu nevoile economice și nu mai respectă cerințele efective de gestionare a riscurilor.
	Gestionarea inadecvată a ciclului de viață și a patch-ului	Absența întreținerii unui inventar adecvat al tuturor activelor TIC în combinație cu practici solide privind gestionarea ciclului de viață și a patch-ului. Aceasta duce la o codificare insuficientă (și, astfel, mai vulnerabilă) a sistemelor TIC și la învechirea acestora, fiind posibil ca acestea să nu mai fie compatibile cu nevoile economice și de administrare a riscurilor.
Riscuri de integritate a datelor TIC	Prelucrarea sau abordarea datelor TIC disfuncționale	Din cauza erorilor sau defecțiunilor la nivel de sistem, comunicare și/sau aplicație, ori din cauza faptului că procesul de extragere, transfer și încărcare a datelor a fost executat eronat, datele ar putea fi corupte sau pierdute.
	Proiectarea eronată a procedurilor de control pentru validarea datelor la sisteme TIC	Erori legate de absența sau ineficiența introducerii automate a datelor sau a procedurilor de control de acceptare (de exemplu, în cazul utilizării datelor externe), a transferului de date, a prelucrării și introducerii procedurilor de control în sisteme TIC (de exemplu, proceduri de control pentru validarea datelor introduse, reconcilieri de date).
	Controlarea deficientă a schimbărilor de date la nivelul producției de sisteme TIC.	Introducerea de erori de date din cauza absenței unor proceduri de control pentru corectitudinea și justificarea acțiunilor de manipulare a datelor efectuate

		la producția de sisteme TIC.
	Proiectarea și/sau gestionarea deficientă a arhitecturii datelor, a fluxurilor de date, a modelelor de date sau a dicționarelor de date	Gestionarea deficientă a arhitecturilor datelor, a modelelor de date, a fluxurilor de date sau a dicționarelor de date poate duce la generarea mai multor versiuni ale aceloraşi date în sistemele TIC, care nu mai sunt consecvente din cauza modelelor de date sau a definițiilor de date aplicate diferit, și/sau a diferențelor la nivelul procesului de generare și schimbare a datelor aferente.
Riscuri de externalizare TIC	Reziliența inadecvată a serviciilor unui terț sau ale unei alte entități din cadrul grupului	Indisponibilitatea serviciilor TIC, serviciilor de telecomunicații și utilități critice externalizate. Pierderea sau coruperea datelor critice/sensibile încredințate furnizorului de servicii.
	Administrarea necorespunzătoare a acțiunii de externalizare	Degradarea avansată a funcționării sau defectarea din cauza unor procese ineficace de pregătire sau control din partea furnizorului de servicii către care s-a realizat externalizarea. Administrarea ineficace a acțiunii de externalizare poate duce la absența competențelor și capacităților adecvate pentru identificarea, evaluarea, atenuarea și monitorizarea integrală a riscurilor TIC și poate limita capacitățile operaționale ale instituțiilor de credit.
	Securitatea inadecvată a unui terț sau a unei alte entități din cadrul grupului	Spargerea sistemelor TIC ale furnizorilor de servicii terți, cu un impact direct asupra serviciilor externalizate sau a datelor critice/confidențiale stocate la furnizorul de servicii. Dobândirea accesului neautorizat de către angajații furnizorului de servicii la date critice/sensibile stocate la furnizorul de servicii.