Cerințe privind Securitatea Informaţiilor & măsuri tehnice și organizatorice pentru Protecţia Datelor

Nivel de protecție Scăzut / Mediu

Măsurile tehnice și organizatorice prezentate aici sunt convenite între DELGAZ GRID SA (numele companiei complet - Client) și _____ (numele complet al companiei - Furnizor).

1 Cerințe privind Securitatea Informațiilor

Cerințele globale sunt cerințe care se aplică, în general, furnizării tuturor serviciilor de către furnizor.

1.1 Surse recunoscute

FURNIZORUL **se asigură că produsele hardware și software sunt obținute din surse cunoscute și renumite și că există un suport tehnic fiabil și un lanț de aprovizionare trasabil.**

1.2 Guvernanța în domeniul securității

FURNIZORUL stabilește, menține și monitorizează un cadru de guvernanță în materie de securitate a informațiilor, care permite organului de conducere al furnizorilor să stabilească o direcție clară și să demonstreze angajamentul său față de securitatea informațiilor și gestionarea riscurilor.

1.3 Managementul Riscurilor Informaționale

FURNIZORUL se asigură că (i) înainte de implementarea unor noi medii IT care găzduiesc informații ale CLIENTULUI inclusiv date cu caracter personal (denumite în continuare „informațiile CLIENTULUI", (ii) înainte de implementarea unor modificări majore la cele existente, și (iii) introducerea unor noi tehnologii semnificative, riscurile de securitatea informațiilor asociate sunt evaluate, tratate, monitorizate și păstrate în limite acceptabile. Informațiile referitoare la activitățile de gestionare a riscurilor sunt partajate fără întârziere cu CLIENTUL, la cerere.

1.4 Managementul Securității

FURNIZORUL (i) a stabilit o funcție de specialist în securitatea informațiilor, condusă de un manager cu puteri decizionale suficiente, căruia îi sunt încredințate autoritatea și resursele adecvate pentru a asigura aplicarea eficientă și consecventă a bunelor practici privind securitatea informațiilor în întreaga companie şi pentru a asigura respectarea cerințelor juridice, de reglementare și contractuale care afectează securitatea informațiilor. FURNIZORUL (ii) menține un program cuprinzător, actualizat, de conștientizare în domeniul securității informațiilor, pentru a promova și a integra comportamentul așteptat privind securitatea în raport cu toate persoanele care au acces la informațiile CLIENTULUI.

1.5 Proceduri Operaționale Documentate

FURNIZORUL a stabilit responsabilități și proceduri pentru administrarea și operarea serviciilor sale, pentru a se asigura că această documentație este (i) conformă cu standardele din industrie și bunele practici recunoscute, (ii) documentată în mod adecvat în scris și (iii) actualizată în orice moment în cursul aplicării prezentului Acord. Documentația privind procedurile de operare va fi partajată cu CLIENTUL la cerere, fără întârziere.

1.6 Managementul activelor

FURNIZORUL se asigură că (i) activele (hardware și software, denumite în continuare „active") care sunt folosite pentru a crea, procesa, stoca sau transmite informațiile CLIENTULUI sunt protejate împotriva coruperii, pierderilor, furtului și divulgării neautorizate pe tot parcursul ciclului lor de viață. Furnizorul se asigură că aceste active sunt înregistrate într-un registru care este: (ii) protejat împotriva modificărilor neautorizate, (iii) actualizat, (iv) copiat periodic (backup) și (v) conține detaliile necesare privind activele și include - dacă este cazul - cerințele de

conformitate referitoare la active. FURNIZORUL se asigură că (vi) toate activele sunt alocate unui proprietar care este responsabil pentru operarea (exploatarea) activului.

1.7 Securitate fizică

FURNIZORUL trebuie să ia măsurile de precauție adecvate pentru securitatea fizică și protecția accesului. În special, trebuie puse în aplicare măsuri pentru protecția împotriva incendiilor și a inundațiilor, protecția împotriva sau pentru evitarea temperaturilor extreme (aer condiționat), alimentarea de rezervă cu energie pentru urgențe.. Accesul la zone cu informații sau sisteme care prelucrează informațiile CLIENTULUI sau procese de suport care afectează securitatea informațiilor CLIENTULUI trebuie să fie limitat la un grup autorizat de persoane (cel mai mic privilegiu). Aceasta include, de asemenea, măsuri de protecție a accesului pentru centrele de date, inclusiv monitorizarea zonelor critice, jurnalele de acces, accesul de către angajații externi companiei se face numai dacă este însoțit și măsuri de securitate împotriva intruziunii.

1.8 Accesul la sistem

FURNIZORUL restricționează accesul la activele în care informațiile CLIENTULUI sunt create, procesate, stocate sau transmise persoanelor autorizate în scopuri comerciale specifice. Aceasta include cel puțin faptul că (i) doar utilizatorii autorizați pot avea acces la informațiile CLIENTULUI; (ii) privilegiile de acces sunt limitate la funcționalitatea aprobată a sistemului; (iii) există o separare adecvată a sarcinilor; (iv) privilegiile de acces nu sunt atribuite colectiv (numele de utilizator și parolele să poată fi partajate). FURNIZORUL se asigură că accesul administrativ la sistemele care stochează sau procesează informațiile CLIENTULUI este (v) limitat la un număr minim de administratori, (vi) protejat prin procedura de autentificare în doi pași sau în cazul în care autentificarea în doi pași nu este posibilă din punct de vedere tehnic, măsuri de securitate echivalente (de ex. parole generate temporar în sistemele de management). FURNIZORUL se asigură de asemenea că accesul administrativ este (vii) întotdeauna înregistrat pentru a permite detectarea și investigarea accesului neautorizat și a manipulării neautorizate a informațiilor CLIENTULUI. (viii) Mai mult decât atât, Furnizorul se asigură că există o procedură oficială in vigoare, care descrie modul în care sunt create, revizuite în mod regulat, modificate, blocate și șterse rolurile, conturile, drepturile de acces și privilegiile privind accesul administrativ.

1.9 Managementul Sistemului

FURNIZORUL administrează sisteme care creează, stochează, procesează sau transmit informații ale CLIENTULUI pentru a (i) face față volumului de muncă curent și preconizat și (ii) le configurează într-o manieră consecventă și precisă pentru a le proteja pe ele și informațiile CLIENTULUI pe care le procesează, stochează sau transmite, împotriva funcționării defectuoase, atacului cibernetic, divulgării neautorizate, coruperii, furtului și pierderii. FURNIZORUL gestionează securitatea sistemelor prin (iii) efectuarea de copii de rezervă a informațiilor esențiale și a software-ului, (iv) aplicarea unui proces riguros de gestionare a modificărilor și (v) monitorizarea acordurilor la nivel de servicii convenite.

1.10 Rețele și comunicații

FURNIZORUL asigură proiectarea rețelelor fizice, wireless și, dacă este cazul, a reţelelor de voce, pentru ca acestea să fie (i) fiabile și rezistente, (ii) să împiedice accesul neautorizat, (iii) să utilizeze conexiuni criptate și (iv) să detecteze traficul suspect. (v) FURNIZORUL asigură configurarea dispozitivelor de rețea (inclusiv routere, firewall-uri și puncte de acces wireless) pentru a funcționa conform cerințelor și pentru a preveni actualizările neautorizate şi incorecte. FURNIZORUL asigură protejarea sistemelor de comunicații electronice prin (vi) stabilirea politicii de utilizare a acestora, (vii) configurarea setărilor de securitate, (viii) securizarea infrastructurii tehnice de sprijin. (ix) Furnizorul asigură ascunderea numelor computerelor și a rețelelor și a topologiilor față de terți. Furnizorul se asigură că restricționează accesul extern la sistemele și rețelele informatice prin (x) stabilirea zonelor demilitarizate (DMZ) între rețelele nesecurizate și rețelele interne, (xi) rutarea traficului de rețea prin firewall-uri sau firewall-uri

proxy, (xii) limitarea metodelor de conectare la minimul necesar, (xiii) acordarea accesului doar la aplicațiile de business autorizate, la sistemele informatice sau la anumite părți ale rețelei.

1.11 Managementul Securității Tehnice

FURNIZORUL instalează soluții de protecție împotriva programelor malware pe sisteme în care informațiile CLIENTULUI pot fi expuse la programe malware, inclusiv (i) servere (de exemplu servere de aplicații, servere de baze de date, servere de fișiere, servere de printare, servere web), (ii) tehnică de calcul (de exemplu computere de tip desktop, laptopuri și alte dispozitive mobile) și (iii) echipamente de birou (de exemplu imprimante de rețea, fotocopiatoare, dispozitive multifuncționale). (iv) Software-ul de protecție împotriva programelor malware trebuie să protejeze împotriva tuturor formelor de malware (de exemplu viruși, viermi, troieni, spyware, rootkit-uri, software-ul botnet, loggers de tip keystroke, ransomware). (v) Software-ul de protecție împotriva malware-ului trebuie distribuit automat și într-un interval de timp definit. FURNIZORUL se asigură și revizuiește periodic dacă (vi) software-ul de protecție împotriva malware-ului nu a fost dezactivat sau funcționalitatea minimizată, (vii) configurația software-ului de protecție împotriva programelor malware este corectă, (viii) actualizările sunt aplicate corect, într-un interval de timp definit, (ix) scanările sunt efectuate la intervale de timp predeterminate și (x) se furnizează o notificare adecvată a evenimentelor malware identificate.

1.12 Separarea Sistemelor de Testare și Productiv

FURNIZORUL se asigură că (i) sistemele de testare și productive sunt cel puțin izolate logic, astfel încât să se reducă riscul accesului neautorizat sau al modificării neautorizate a sistemelor productive. (ii) În cazul în care separarea nu este posibilă, FURNIZORUL se asigură că va stabili proceduri modificate special pentru procesul de Solicitare Schimbări și în vederea gestionării incidentelor și situațiilor de urgență pentru a permite reacții rapide și adecvate la perturbări și problemele legate de sistemele productive. (iii) Datele productive nu sunt permise în medii de testare sau de dezvoltare și trebuie anonimizate dacă conțin date cu caracter personal sau date de identificare a persoanelor.

1.13 Dezvoltarea/ achiziționarea de software

FURNIZORUL se asigură că software-ul dezvoltat intern sau software-ul achiziționat extern, utilizat pentru procesarea, stocarea sau transmiterea informațiilor Clientului, nu este vulnerabil în ceea ce privește "OWASP TOP Ten" și "SANS Top 25 Errors of the Most Dangerous Software".

1.14 Scanarea de Vulnerabilități

FURNIZORUL se asigură că (i) sistemele accesibile în mod public sunt testate în mod regulat (cel puțin lunar) împotriva vulnerabilităților și a defecțiunilor de configurare prin efectuarea de teste dinamice (teste de penetrare sau scanări de vulnerabilități). (ii) Toate rezultatele acestor teste relevante pentru CLIENT sunt partajate cu CLIENTUL fără întârziere; (iii) vulnerabilitățile critice vor fi raportate către CLIENT imediat. (iv) FURNIZORUL oferă asistență și sprijin pentru auditul patch-urilor de securitate și a managementului vulnerabilităților realizat de CLIENT. (v) Atenuarea vulnerabilităților de securitate va fi efectuată pe baza nivelului de risc și a intervalelor de timp convenite între părți.

1.15 Nivele de patch-uri actualizate

FURNIZORUL asigură remedierea vulnerabilităților tehnice prin administrarea unui proces de gestionare a patch-urilor care asigură (i) identificarea și obținerea de patch-uri din surse autorizate, imediat ce acestea sunt disponibile, (ii) decizia când pot fi distribuite patch-urile, (iii) patch-uri de testare pe baza unor criterii cunoscute, (iv) distribuirea patch-urilor în timp util, (v) înregistrarea de patch-uri care au fost aplicate într-o baza de date de management al configurarilor (CMDB). (v) FURNIZORUL este împuternicit să aplice patch-uri în mediul IT, inclusiv

hipervizoare de virtualizare, mașini virtuale, sisteme de operare și aplicații, atâta timp cât acest lucru nu are un impact negativ asupra confidențialității, integrității sau disponibilității informațiilor CLIENTULUI.

1.16 Cerințe Minime de Autentificare

FURNIZORUL se asigură că cerințele minime ale CLIENTULUI pentru autentificare (autentificarea în doi paşi) sunt impuse prin intermediul soluției CLIENTULUI "Federated Single Sign-On" pentru mediul IT operat pentru a stoca sau procesa informațiile CLIENTULUI. Trebuie aplicate principiile celor mai puține privilegii, al necesității de a cunoaşte şi de separare a sarcinilor. Mai mult, trebuie aplicat un model de control al accesului bazat pe roluri.

1.17 Cerințe de Proiectare a Rețelei

Trebuie să existe o arhitectură multi-nivel și un DMZ (zonă demilitarizată) pentru aplicații accesibile din Internet. Segmentele de rețea trebuie să fie separate de segmentele de nivel scăzut și mediu cu măsuri de securitate adecvate pentru a preveni traficul de date între segmente. Segmentul de rețea pentru nivelul foarte ridicat ar trebui, de preferință, să fie, de asemenea, separat și securizat față de segmentele pentru nivelurile ridicate.

1.18 **Accesul** de la distanță și munca din afara biroului

FURNIZORUL se asigură că posibilitățile de acces la distanță sunt protejate în conformitate cu cele mai curente tehnici. Munca din afara biroului a angajaților FURNIZORULUI care au acces la informațiile CLIENTULUI trebuie notificată în prealabil CLIENTULUI și poate avea loc numai cu condiția ca angajații să fi fost instruiți și să își fi asumat în scris respectarea reglementărilor privind protecția datelor și cele de operare. FURNIZORUL va pune la dispoziția angajaților săi software și hardware în acest scop, care pot fi utilizate numai în scopuri de business sau care acceptă o separare eficientă a datelor de business și cele private (de exemplu, soluții bazate pe containere securizate). Documentele confidențiale trebuie păstrate în siguranță în ceea ce privește accesul terților; documentele pot fi distruse/ eliminate numai la sediul FURNIZORULUI în cadrul stabilit pentru eliminare/ distrugere în conformitate cu reglementările privind protecția datelor. Măsurile de securitate convenite trebuie, de asemenea, observate atunci când se oferă serviciul accesabil prin muncă din afara biroului. Ascultarea și citirea de către persoane neautorizate trebuie excluse. FURNIZORUL va oferi CLIENTULUI, la cerere, toate informațiile necesare pentru a dovedi conformitatea cu specificațiile pentru munca din afara biroului.

1.19 Criptarea

Datele în repaus și datele în mișcare (în tranzit) vor fi stocate și transmise numai utilizând protocoale securizate și criptare de ultimă generație. Funcțiile de autentificare (parole, PIN-uri) pot fi transmise doar criptate prin rețea. În plus, transporturile fizice ale dispozitivelor de stocare trebuie să fie securizate prin protecție fizică și criptare.

1.20 Securizare (Hardening)

Toate sistemele informatice și de rețea trebuie securizate. Aceasta include (i) dezactivarea aplicațiilor, serviciilor, instrumentelor, protocoalelor și interfețelor inutile, (ii) ștergerea sau cel puțin schimbarea numelor de utilizator și a parolelor livrate de furnizori, (iii) activarea opțiunilor de sporire a securității și (iv) prevenirea transferului de informații tehnice către entități externe.

1.21 Înregistrarea evenimentelor de securitate:

Pentru a permite detectarea și investigarea accesului neautorizat și a manipulării neautorizate a informațiilor CLIENTULUI, FURNIZORUL se asigură că (i) înregistrarea evenimentelor este activată permanent pentru toate sistemele operate de acesta pentru a crea, stoca, procesa sau transmite informațiile CLIENTULUI, (ii) sistemele sunt configurate astfel încât să genereze evenimente legate de securitate și evenimente cu relevanță pentru integritatea datelor (inclusiv tipuri de evenimente cum ar fi modificări ale informațiilor CLIENTULUI, încercările de conectare reușită și nereușită a utilizatorilor, crearea/ modificarea/ ștergerea serviciului, crearea/ modificarea/

ștergerea obiectelor, disfuncționalitatea sistemului, ștergerea conturilor de utilizator) precum şi atributele asociate fiecărui eveniment (de exemplu data, ora, ID-ul utilizatorului, numele fișierului și adresa IP), (iii) sursele coerente de date și de timp fiabile asigură că jurnalele de evenimente utilizează mărci temporale precise (de exemplu: prin utilizarea serverelor NTP), (iv) jurnalele de evenimente de securitate și jurnalele de evenimente cu relevanță pentru integritatea datelor sunt protejate împotriva accesului neautorizat și modificării/ suprascrierii accidentale sau intenționate.

1.22 Eliminarea Securizată și Reutilizarea

FURNIZORUL se asigură că hardware-ul care urmează a fi dezafectat este (i) fie complet șters înainte de a fi reutilizat, vândut sau returnat astfel încât toate informațiile CLIENTULUI să fie șterse în întregime în condiţii de siguranță (ii) sau este distrus în condiţii de siguranță. (iii) Ștergerea completă sau distrugerea trebuie realizată într-un mod securizat, utilizând cele mai moderne tehnologii și practici, cum ar fi instrumentele și practicile definite în NIST 800-88 "Ghid pentru formatarea suporturilor media". (iv) Conceptele pentru eliminarea şi ştergerea securizată, precum și dovezile privind eliminarea și ștergerea securizată a bunurilor informaţionale ale CLIENTULUI sunt partajate cu CLIENTUL, la cerere.

1.23 Securitatea Resurselor Umane

Pentru fiecare persoană care acționează în numele FURNIZORULUI și căreia i se acordă permisiuni de acces (la nivel local sau de la distanță), informațiile de identificare a persoanei trebuie puse la dispoziția CLIENTULUI. FURNIZORUL asigură o verificare personală a identității entităților umane și că nimeni nu abuzează de accesul sau permisiunea acordată persoanelor de către FURNIZOR. În plus, FURNIZORUL își asumă responsabilitatea pentru orice daune produse datorită accesului neautorizat și/ sau utilizării informațiilor CLIENTULUI. FURNIZORUL deleagă doar personalul care este calificat în mod demonstrabil pentru sarcinile necesare.

1.24 Securitatea Lanțului de Aprovizionare

FURNIZORUL asigură identificarea și gestionarea riscurilor aferente informațiilor pe parcursul fiecărei etape a relațiilor cu furnizorii externi de hardware și software în întregul lanț de aprovizionare prin (i) încorporarea cerințelor de securitate privind informațiile în contracte formale și (ii) obținerea asigurării că acestea sunt îndeplinite. (iii) FURNIZORUL se asigură că subcontractanții implicați în prelucrarea, stocarea, transmiterea sau eliminarea informațiilor CLIENTULUI îndeplinesc cel puțin cerințele convenite în prezenta Anexă. (iv) Furnizorul este responsabil pentru asigurarea unei guvernări adecvate a subcontractantului/ subcontractanților, precum și pentru conformitatea controalelor externalizate.

2 Cerințe referitoare la protecția datelor

2.1 Angajamentul de confidențialitate

FURNIZORUL obligă în scris toți angajații care prelucrează date cu caracter personal ale CLIENTULUI sau au acces la aceste date să păstreze confidențialitatea cu privire la prelucrarea datelor cu caracter personal.

Dacă este legat de comandă sau este o cerință legală, FURNIZORUL obligă angajații în scris să păstreze secretul privind telecomunicațiile (în conformitate cu Directiva Europeană nr. 58/2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice – ePrivacy Directive - sau reglementări privind confidențialitatea electronică în versiunea lor validă, coroborat cu normele naționale privind secretul telecomunicațiilor, de exemplu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.

FURNIZORUL va instrui toți angajații care prelucrează date cu caracter personal ale CLIENTULUI sau au acces la aceste date în ceea ce privește securitatea datelor și protecția datelor. Participarea va fi documentată pe bază de nume specific.

2.2 Protecția datelor prin design

Furnizorul va stabili reglementări privind „Protecția Datelor în etapa de Design/ dezvoltare" pentru a lua în considerare dreptul la protecția datelor în dezvoltarea și proiectarea produselor, serviciilor și aplicațiilor (de exemplu, prin măsuri precum minimizarea datelor, pseudonimizarea, setările implicite pentru protecția datelor).

3 Standarde

Furnizorul acceptă să mențină următoarele standarde:

- ISO/IEC 27001: Toate facilitățile de găzduire a datelor și de suport și procesele în care informațiile Clientului sunt stocate sau prelucrate sunt operate în conformitate cu ISO/IEC 27001 "Tehnologia informației – Tehnici de securitate – Sisteme de management a securității informației - Cerințe".
- Furnizorul este de acord să partajeze Declarațiile de Conformitate cu Clientul la cerere.

4 Interfețele proceselor de securitate IT

Ambele părți sunt de acord să comunice și să pună la dispoziție persoane de contact pentru următoarele procese de securitate IT:

- Managementul Conformității: Pentru a schimba informaţii cu privire la respectarea cerințelor, a furniza în mod constant certificate și rapoarte, astfel cum sunt definite în prezenta Anexă, și a discuta și a conveni asupra acțiunilor de gestionare a neconformităților existente și a riscurilor aferente. Răspunsuri sincere la întrebările de „autoevaluare a furnizorului" prin intermediul platformei de gestionare a riscurilor CLIENTULUI.

- Managementul Incidentelor de Securitate IT și breșele privind datele personale: Pentru a schimba informații privind incidentele de securitate IT sau evenimentele de securitate IT care ar putea conduce la un incident de securitate IT care afectează sau ar putea afecta mediul IT utilizat pentru stocarea sau procesarea informațiilor CLIENTULUI. "Managementul incidentelor de securitate IT" include, de asemenea, gestionarea solicitărilor de expertiză/emise de către CLIENT. Breșele privind datele cu caracter personal și incidentele de securitate IT cu relevanță pentru protecția datelor trebuie raportate de FURNIZOR către CLIENT imediat, dar cel puțin în termenul legal stabilit; în acest sens, se face trimitere la dispozițiile relevante ale acordului de protecție a datelor.

- Managementul Riscurilor: Pentru a schimba informaţii privind activitățile de gestionare a riscurilor efectuate de FURNIZOR pentru a asigura identificarea, evaluarea, gestionarea, monitorizarea și menținerea într-o limită acceptabilă, în mod permanent, a riscurilor legate de securitatea informațiilor.

- Managementul Vulnerabilităților: Pentru a schimba informații privind vulnerabilitățile care afectează sau ar putea afecta mediul IT utilizat pentru stocarea sau procesarea informațiilor CLIENTULUI și pentru a discuta și a conveni asupra acțiunilor de atenuare a vulnerabilităților existente.

- Managementul Patch-urilor: Pentru a schimba informații privind ferestrele de mentenanță agreate și distribuirea de patch-uri.

- Managementul Identității și Accesului: Pentru a schimba informații privind subiectele legate de Managementul Identității și Accesului.

Ambele părți sunt de acord să colaboreze și să facă schimb de informații în cadrul fiecăruia dintre procesele de securitate menționate mai sus. Părțile vor conveni asupra unor mijloace tehnice privind schimbul de informații, precum și a indicatorilor-cheie de performanță (KPI) în vederea asigurării conformității cu procedurile de securitate convenite.

Ambele părți sunt de acord că persoanele de contact desemnate pentru procesele de securitate menționate mai sus există și pot fi înlocuite. În cazul înlocuirii, partea care înlocuiește o persoană de contact desemnată va informa prompt cealaltă parte.

Persoană de contact din partea Clientului

Nume şi prenume: Truță Mihai

Adresă de e-mail: cybersecurityro [at] delgaz-grid.ro

Persoană de contact din partea Furnizorului

Nume şi prenume:

Telefon:

Adresă de e-mail:

5 Sistemul de Control Intern orientat către Servicii (ICS)

În cazul în care datelor prelucrate de FURNIZOR li se aplică Controalele Interne ale CLIENTULUI, FURNIZORUL trebuie să respecte cerințele descrise mai jos.

FURNIZORUL asigură proiectarea și eficiența operațională a ICS legate de riscurile IT derivate din descrierea procesului COBIT 5, declarația de intenție, obiectivele și practicile pentru procesele COBIT 5, astfel cum sunt enumerate mai jos:

- APO 01 Managementul Cadrului IT (IT Framework)
- APO08 Managementul Relațiilor
- APO09 Managementul Acordurilor privind Serviciile
- APO10 Managementul Furnizorilor
- APO12 Managementul Riscurilor
- APO13 Managementul Securității
- BAI03 Identificarea și Construirea Soluțiilor
- BAI04 Managementul Disponibilității și Capacității
- BAI06 Managementul Schimbării
- BAI07 Managementul Acceptării Schimbărilor & Tranziției
- BAI09 Managementul Activelor
- BAI10 Managementul Configurărilor
- DSS01 Managementul Operațiunilor
- DSS02 Managementul Solicitări de Servicii şi Incidente
- DSS03 Managementul Problemelor
- DSS05 Managementul Serviciilor de Securitate
- MEA2 Monitorizarea, Evaluarea și Analizarea Sistemului de Control Intern
- MEA3 Monitorizarea, Evaluarea și Analizarea Conformităţii cu Cerinţele Externe

FURNIZORUL va desemna o persoană de contact principală pentru a rezolva problemele legate de ICS.

FURNIZORUL stabilește controalele necesare pentru a răspunde riscurilor IT, de asemenea implementează și operează aceste controale și păstrează evidența operațiunilor de control.

FURNIZORUL pune la dispoziția CLIENTULUI evidențe privind proiectarea și eficacitatea operațională a controalelor, la cererea CLIENTULUI.

FURNIZORUL raportează imediat CLIENTULUI toate deficiențele ICS și remedierea acestora.

FURNITORUL prezintă un raport anual de asigurare privind controalele orientate spre servicii la organizația FURNIZORULUI în conformitate cu Standardul Internațional privind Angajamentele de Asigurare (ISAE 3402), Tipul II sau un standard echivalent până la sfârșitul anului.