European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

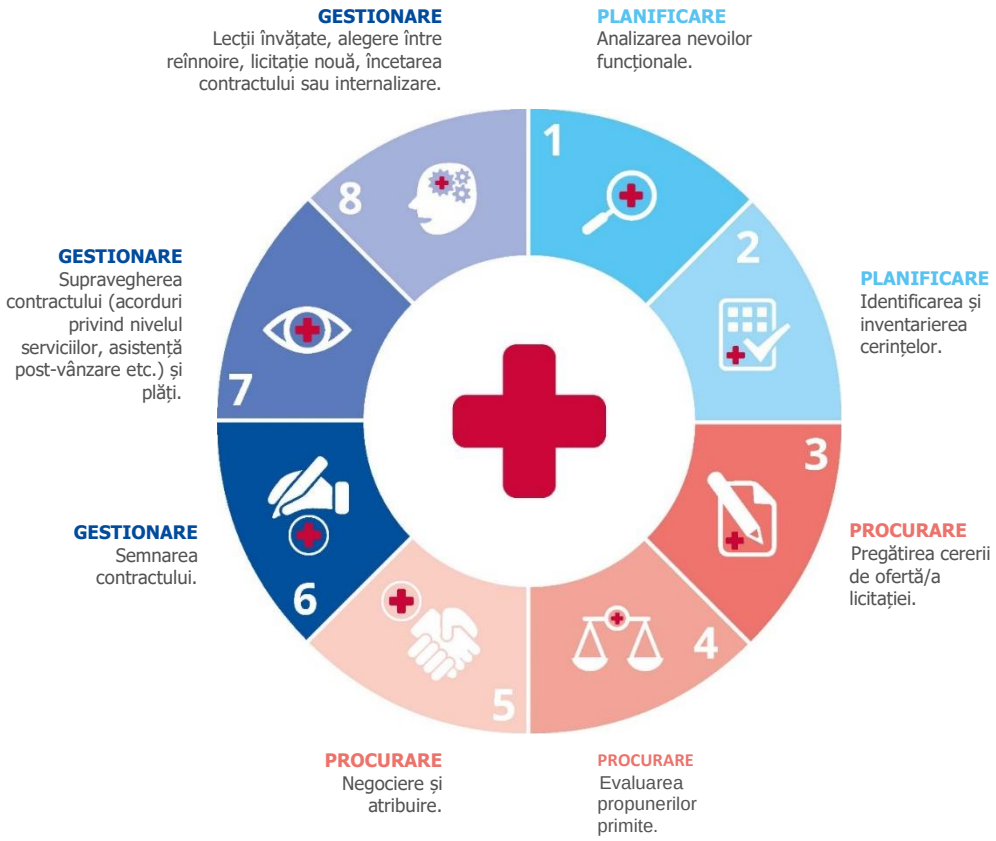
GHID DE ACHIZIȚII PUBLICE PENTRU SISTEME DE SECURITATE CIBERNETICĂ ÎN SPITALE

Raportul își propune să fie un „ghid” pentru personalul medico-sanitar. Multe din practicile și recomandările menționate în el vor fi utile și altor organizații din domeniul sănătății, deoarece procesele de achiziții publice pot fi în mare măsură similare. Ghidul este util personalului medico-sanitar cu funcții tehnice în spitale, și anume personalului executiv cu funcții de conducere: responsabil sisteme informatice (CIO), responsabil de securitatea sistemelor informatice (CISO), responsabil tehnic (CTO), precum și echipelor IT și responsabililor cu achizițiile publice din organizațiile din domeniul sănătății. Documentul de față prezintă pe scurt elementele principale ale raportului – pentru mai multe detalii, cititorul trebuie să revină la publicația ENISA: Bunele practici ale ENISA pentru securitatea serviciilor de sănătate, publicată în februarie 2020.

PROCESUL DE ACHIZIȚII PUBLICE

Întrucât ecosistemul spitalelor cuprinde mai multe componente IT, securitatea cibernetică ar trebui examinată separat în toate aceste componente diferite. Securitatea cibernetică ar trebui să facă parte integrantă din diversele etape ale procesului de achiziții publice. În această secțiune prezentăm etapele comune ale procesului de achiziții publice pentru obținerea de produse și servicii precum dispozitive medicale, sisteme și infrastructuri informatice.

Figura 1: Ciclul de viață al procesului de achiziții publice în cadrul spitalelor



- Etapa de planificare: Inițial, spitalul își analizează nevoile și inventariază pe plan intern cerințele mai multor departamente. De exemplu, în cazul obținerii unui nou serviciu de tip cloud, CTO ar trebui să identifice nevoile și să înțeleagă tipul de utilitate oferit de acest serviciu.

- Etapa de procurare: În continuare, cerințele sunt transpuse în specificații tehnice și, în colaborare cu biroul de achiziții publice, începe procesul procurării lor (de exemplu, se publică o licitație). Spitalul primește ofertele desemnate, comitetul (din care face parte CTO/CISO și/sau un membru al echipei IT) evaluează ofertele și selectează produsele cele mai adecvate. Se desfășoară negocieri cu contractantul și se atribuie contractul.

- Etapa de gestionare: În etapa finală, contractul (gestionare și monitorizare) este alocat responsabilului de proiect din cadrul spitalului. Persoana desemnată are sarcina de a închide licitația și de a primi orice feedback din partea utilizatorilor cu privire la performanța reală a echipamentului/sistemului/serviciului.

TIPURI DE ACHIZIȚII PUBLICE ÎN SPITALE

Tabelul 1: Tipuri de achiziții publice (taxonomia activelor)

Tip de achiziție	Descrierea tipului
Sisteme informatice clinice	Cuprinde achiziția oricărui tip de software orientat spre îngrijiri medicale
Dispozitive medicale	Orice echipament hardware destinat tratării, ținerii sub control sau diagnosticării bolilor
Echipamente de rețea	Cabluri de rețea (coaxiale, optice), gateway-uri, routere, switchuri, firewalluri, VPN, IPS, IDS etc.
Sisteme de îngrijire la distanță	Instalații sau dispozitive pentru furnizarea de asistență medicală în afara mediului spitalicesc, în special prin ceea ce este denumit în prezent „servicii de asistență spitalicească la domiciliu”
Dispozitive mobile pentru clienți	Toate programele informatice care oferă asistență medicală sau colectare de date medicale fără a fi conectate direct la rețeaua spitalicească; de exemplu: aplicații de telemedicină
Sisteme de identificare	Sisteme de identificare unică a pacienților sau a personalului medical (scanere biometrice, cititoare de carduri etc.) și de garantare a identificării și/sau a autorizării accesului la sistemele informatice
Sisteme de gestionare a clădirilor	Orice tip de construcție în care se pot amplasa unități medicale
Sisteme de control industrial	Sisteme care controlează toate aspectele fizice ale centrelor, precum sisteme de reglare a puterii, sisteme de blocare a ușilor, sisteme de securitate cu circuit închis
Servicii profesionale	Toate tipurile de servicii, externalizate sau nu, furnizate de profesioniști sau de societăți comerciale: servicii medicale, transport, contabilitate, inginerie, IT, juridic, întreținere, curățenie, servicii de alimentație publică etc.
Servicii de tip cloud	Orice sistem informatic și de comunicații sau alt sistem informatic care nu este amplasat în clădirea unității medicale sau într-un centru de date aflat sub controlul complet al departamentului IT al centrului medical

TAXONOMIA AMENINȚĂRILOR

Diferitele tipuri de achiziții sunt asociate cu diferite amenințări la adresa mediului TIC dintr-un spital. Consultați taxonomia amenințărilor prezentată în această secțiune împreună cu departamentul IT, de securitate sau de risc, pentru a identifica amenințările cele mai relevante pentru organizația dumneavoastră. Această activitate ar trebui să facă parte din sarcinile echipei IT a spitalului, indiferent de potențialul de achiziții publice.

Tabelul 2: Tipuri de amenințări (taxonomia amenințărilor)

Amenințare	Exemple
Fenomene naturale	Incendii, inundații sau cutremure
Probleme în lanțul de aprovizionare	Probleme la furnizorul de servicii de tip cloud, probleme la furnizorul de rețea, întreruperea alimentării cu energie electrică, probleme sau neasumarea răspunderii din partea producătorului dispozitivului medical
Erori umane	Eroare de configurare a sistemului medical, absența registrelor de audit, controlul accesului neautorizat/lipsa procedurilor, neconformitate (BYOD – *Bring Your Own Device* – când angajaților li se permite să utilizeze echipamentele proprii), eroare a personalului medical sau a pacientului
Acțiuni rău-intenționate	Malware (virus, ransomware, BYOD), hijack (cryptojacking, medjacking), inginerie socială (phishing, baiting, clonarea dispozitivelor), furt (de date, de dispozitive), modificare ilicită a dispozitivelor medicale, skimming (furt de date de pe carduri bancare), refuzul serviciului, atacuri web, atacuri asupra aplicațiilor web, amenințări interne, manipulare/deteriorare fizică, furt de identitate, spionaj cibernetic, perturbarea funcționării componentelor mecanice
Defecțiuni de sistem	Probleme de software, firmware învechit, defectarea dispozitivelor, defectarea componentelor rețelei, întreținere insuficientă

BUNE PRACTICI ÎN MATERIE DE SECURITATE CIBERNETICĂ ÎN DOMENIUL ACHIZIȚIILOR PUBLICE

Lista de bune practici de mai jos nu este în niciun caz exhaustivă, însă oferă un avantaj solid informaticianului medical responsabil cu achiziționarea de echipamente într-un spital. Setul de bune practici este rezultatul colectiv al tuturor contribuțiilor primite de la personalul medico-sanitar intervievat. Cititorul poate adapta lista în funcție de prioritățile organizației sale.

BP 1. Implicarea departamentului IT în diferitele etape ale procedurii de achiziții publice, pentru a se ține seama de expertiza sa în ceea ce privește aspectele de securitate cibernetică.

Etapele procesului de achiziții: Toate

Tipuri de achiziții asociate: Toate

Amenințări asociate: Toate

BP 2. Implementarea unui proces de identificare și gestionare a vulnerabilităților pentru a se asigura luarea lor în considerare înainte de achiziționarea de noi produse sau servicii și monitorizarea vulnerabilităților produselor/serviciilor existente pe parcursul întregului lor ciclu de viață.

Etapele procesului de achiziții: Toate

Tipuri de achiziții asociate: Sisteme de informații clinice, dispozitive medicale, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Toate

BP 3. Elaborarea unei politici privind actualizările hardware și software, pentru a asigura aplicarea celor mai recente corecții la sistemul de operare și la software și menținerea unui program antivirus actualizat.

Etapele procesului de achiziții: Toate

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 4. Consolidarea controalelor de securitate la comunicațiile wireless, pentru asigurarea unui acces limitat și strict controlat la rețelele Wi-Fi ale spitalului.

Etapele procesului de achiziții: Toate

Tipuri de achiziții asociate: Dispozitive medicale, dispozitive client la distanță, sisteme de identificare, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, erori umane

BP 5. Stabilirea unor politici de testare pentru a se asigura că produsele nou achiziționate sau nou configurate sunt supuse unui test de penetrare, iar măsurile de remediere luate sunt în conformitate cu parametrii operaționali din mediul real.

Etapele procesului de achiziții: Toate

Tipuri de achiziții asociate: Sisteme de informații clinice, dispozitive medicale, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de gestionare a clădirilor, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, defecțiuni de sistem, erori umane

BP 6. Instituirea unor planuri de continuitate a activității pentru ca defectarea unui sistem să nu perturbe serviciile de bază ale spitalului și pentru ca rolul furnizorului să fie bine definit.

Etapele procesului de achiziții: Toate

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 7. Luarea în considerare a aspectelor legate de interoperabilitate, pentru a se evita problemele de securitate la conexiunea cu componentele deja existente (IT moștenit).

Etapele procesului de achiziții: Toate

Tipuri de achiziții asociate: Sisteme de informații clinice, dispozitive medicale, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Defecțiuni de sistem, erori umane, acțiuni rău-intenționate

BP 8. Posibilitatea testării tuturor componentelor, pentru a garanta că acestea funcționează conform specificațiilor: verificarea ușurinței de utilizare, verificarea corectitudinii rezultatelor în regim de încărcare și verificarea deficiențelor de securitate (politică deficitară privind parolele, atacuri de tip SQL injection).

Etapele procesului de achiziții: Toate

Tipuri de achiziții asociate: Sisteme de informații clinice, dispozitive medicale, dispozitive client la distanță, sisteme de identificare, servicii de tip cloud, sisteme de control industrial, sisteme de îngrijire la distanță, sisteme de gestionare a clădirilor, dispozitive mobile pentru clienți

Amenințări asociate: Acțiuni rău-intenționate, erori umane, deficiențe de sistem, probleme în lanțul de aprovizionare

BP 9. Permiterea auditării și a înregistrării în jurnale în vederea urmăririi atacatorilor și a cantității de informații pierdute/furate la compromiterea sistemului.

Etapele procesului de achiziții: Toate

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 10. Criptarea datelor sensibile cu caracter personal staționare și în tranzit, prin definirea unei politici pentru sistemele, serviciile sau dispozitivele care prelucrează categoriile speciale de date cu caracter personal prevăzute la articolul 9 din RGPD.

Etapele procesului de achiziții: Toate

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 11. Efectuarea unei evaluări a riscurilor ca parte a procesului de achiziții publice.

Etapele procesului de achiziții: Planificare

Tipuri de achiziții asociate: Toate

Amenințări asociate: Toate

BP 12. Planificarea în avans a cerințelor hardware, de rețea și privind licențele, pentru a stabili dacă sunt necesare actualizări și/sau achiziții suplimentare înainte de instalarea noului sistem.

Etapele procesului de achiziții: Planificare

Tipuri de achiziții asociate: Sisteme de informații clinice, echipamente de rețea, sisteme de identificare, sisteme de control industrial

Amenințări asociate: Probleme în lanțul de aprovizionare, defecțiuni de sistem, fenomene naturale, erori umane

BP 13. Identificarea amenințărilor legate de achizițiile de produse sau servicii și asigurarea identificării continue a amenințărilor pe parcursul ciclului de viață al componentelor achiziționate.

Etapele procesului de achiziții: Planificare, gestionare

Tipuri de achiziții asociate: Toate

Amenințări asociate: Toate

BP 14. Separarea rețelei pentru a asigura posibilitatea izolării și/sau a filtrării traficului în rețea în scopul limitării și/sau prevenirii accesului între diferitele zone ale rețelei.

Etapele procesului de achiziții: Planificare, procurare

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 15. Stabilirea cerințelor de rețea pentru a asigura interoperabilitatea și a evita lacunele după crearea topologiei rețelei și a componentelor.

Etapele procesului de achiziții: Planificare

Tipuri de achiziții asociate: Sisteme de informații clinice, echipamente de rețea, sisteme de identificare, sisteme de control industrial, servicii de tip cloud, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți

Amenințări asociate: Probleme în lanțul de aprovizionare, defecțiuni de sistem, fenomene naturale

BP 16. Stabilirea cerințelor de bază în materie de securitate și transpunerea lor în criterii de eligibilitate la selectarea furnizorilor.

Etapele procesului de achiziții: Planificare, procurare

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 17. Crearea unei cereri de ofertă specifice pentru achiziționarea serviciilor de tip cloud, ținând seama de cerințele normative și de politică.

Etapele procesului de achiziții: Planificare, procurare

Tipuri de achiziții asociate: Servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare

BP 18. Acordarea de prioritate achiziționării de active certificate în conformitate cu sistemele/standardele de securitate cibernetică.

Etapele procesului de achiziții: Procurare

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 19. Efectuarea de evaluări ale impactului asupra protecției datelor atunci când se planifică achiziționarea unui nou sistem sau serviciu.

Etapele procesului de achiziții: Procurare

Tipuri de achiziții asociate: Sisteme de informații clinice, dispozitive medicale, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, servicii profesionale, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, erori umane

BP 20. Instalarea de gateway-uri care să mențină conectate sistemele/mașinile moștenite și să asigure controlul la frontieră în cazul unor probleme în interiorul acestor grupuri.

Etapele procesului de achiziții: Procurare, gestionare

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 21. Asigurarea de formare în domeniul securității cibernetice cu privire la practicile de securitate ale organizației, pentru o instruire corespunzătoare a personalului intern sau a contractanților/consultanților externi care lucrează în unitate.

Etapele procesului de achiziții: Procurare, gestionare

Tipuri de achiziții asociate: Toate

Amenințări asociate: Acțiuni rău-intenționate, erori umane

BP 22. Elaborarea unor planuri de intervenție în caz de incidente, care să includă produsele sau sistemele nou achiziționate.

Etapele procesului de achiziții: Procurare, gestionare

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 23. Implicarea vânzătorului/producătorului în gestionarea incidentelor și stabilirea unor condiții clare în cererea de ofertă.

Etapele procesului de achiziții: Procurare, gestionare

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 24. Programarea și monitorizarea operațiunilor de întreținere pentru toate echipamentele, pentru a se asigura un nivel adecvat de funcționalitate și pentru a decide cu privire la eventualele actualizări/corecții etc.

Etapele procesului de achiziții: Procurare, gestionare

Tipuri de achiziții asociate: Sisteme de informații clinice, echipamente de rețea, dispozitive medicale, sisteme de gestionare a clădirilor, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Eroare umană, defecțiuni de sistem, fenomene naturale

BP 25. Reducerea la minimum a accesului de la distanță și administrarea acestuia astfel încât comunicațiile externe cu furnizorul să se limiteze doar la dispozitivul pe care acesta trebuie să îl controleze.

Etapele procesului de achiziții: Procurare, gestionare

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem, erori umane

BP 26. Solicitarea de corecții pentru toate componentele și includerea informațiilor în cererea de ofertă.

Etapele procesului de achiziții: Procurare, gestionare

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem

BP 27. Sensibilizarea personalului cu privire la securitatea cibernetică, pentru ca angajații să fie conștienți de riscurile asociate produselor sau serviciilor nou achiziționate.

Etapele procesului de achiziții: Gestionare

Tipuri de achiziții asociate: Toate

Amenințări asociate: Toate

BP 28. Inventarierea activelor și gestionarea configurațiilor, pentru a se asigura actualizarea corespunzătoare a inventarului atunci când se adaugă sau se elimină orice componentă din mediul TIC, precum și existența și gestionarea corespunzătoare a configurațiilor de securitate de bază pentru componentele TIC.

Etapele procesului de achiziții: Gestionare

Tipuri de achiziții asociate: Sisteme de informații clinice, dispozitive medicale, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare

Amenințări asociate: Acțiuni rău-intenționate, erori umane, defecțiuni de sistem

BP 29. Instituirea unor mecanisme specifice de control al accesului în incintele cu dispozitive medicale, care ar trebui să fie de asemenea protejate din punct de vedere fizic și accesibile numai personalului specializat.

Etapele procesului de achiziții: Gestionare

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de gestionare a clădirilor, sisteme de identificare

Amenințări asociate: Acțiuni rău-intenționate, erori umane

BP 30. Programarea testelor de penetrare în mod frecvent sau după o modificare a arhitecturii/sistemului și includerea condițiilor aferente în cererea de ofertă.

Etapele procesului de achiziții: Procurare, gestionare

Tipuri de achiziții asociate: Dispozitive medicale, sisteme de informații clinice, echipamente de rețea, sisteme de îngrijire la distanță, dispozitive mobile pentru clienți, sisteme de identificare, sisteme de control industrial, servicii de tip cloud

Amenințări asociate: Acțiuni rău-intenționate, probleme în lanțul de aprovizionare, defecțiuni de sistem