Cum sa structurati cat mai bine evidentele de audit si cum sa implementati natural procedurile operationale?

- Identificati sistemele/echipamentele informatice si serviciile critice. Evaluati sistemele/echipamentele informatice si serviciile care stau la baza furnizarii serviciilor esentiale pentru a determina care dintre acestea sunt critice
- Documentati fiecare sistem/echipament informatic si serviciu critic, inclusiv informatii despre configuratia acestora si despre modul in care functioneaza
- Identificati riscurile: faceti analiza de riscuri pentru sistemele critice identificate
- Creati proceduri si planuri de lucru pentru a preveni sau a minimiza riscurile identificate
- Monitorizați continuu sistemele și serviciile critice pentru a verifica dacă acțiunile planificate funcționează și testați periodic sistemele pentru a verifica dacă acestea sunt în siguranta

Pentru a implementa proceduri operationale eficiente:

- Definiti si documentati procedurile clare pentru fiecare aspect esential al sistemelor si serviciilor critice, cum ar fi gestionarea incidentelor de securitate, back-up-ul si recuperarea de la dezastre.
- Asigurati-va ca procedurile sunt actualizate si testate periodic pentru a se asigura ca sunt eficiente
- Instruiti si informati personalul despre procedurile operationale si asigurati-va ca acestia inteleg rolul lor in implementarea acestora.
- Monitorizati si evaluati periodic eficacitatea procedurilor operationale si luati masurile necesare pentru a le imbunatati.

Exemplu cerinte din Ordin 559/2021, Anexa 9

[CAS1]. Cerințe specifice auditului arhitecturii

(1) **Acțiuni ale OE.** Operatorul economic trebuie să furnizeze auditorului de securitate cibernetică elementele de arhitectură și configurare a rețelelor și sistemelor informatice auditate.

(2) **Acțiuni tehnice ale ASI.** Auditorul de securitate cibernetică trebuie să:

- ✓ Revizuiască/auditeze următoarele documente atunci când acestea există:
  - ➢ diagramele arhitecturale de nivel 2 și 3 corespunzătoare Modelului OSI (Interconectarea Sistemelor Deschise / Open Systems Interconnection);
  - ➢ matricea fluxurilor;
  - ➢ regulile de filtrare;
  - ➢ configurarea echipamentelor de rețea (routere și comutatoare)
  - ➢ interconectări cu rețele terțe sau Internet;
  - ➢ analizele de risc ale rețelelor și sistemelor informatice;
  - ➢ documentele de arhitectură tehnică legate de ținta auditului.

[CAS2]. Cerințe specifice auditului de configurare

(1) **Acțiuni ale OE.** Operatorul economic trebuie să furnizeze auditorului de securitate cibernetică elementele de configurare ale rețelelor și sistemelor informatice auditate. Elementele de configurare pot fi identificate manual sau automat, folosind "acces privilegiat", sub formă de fișiere de configurare sau capturi de ecran.

Această acțiune poate fi întreprinsă direct de auditorul de securitate cibernetică după aprobarea operatorului economic supus auditului.

(2) **Acțiuni tehnice ale ASI.** Auditorul de securitate cibernetică trebuie să:

- ✓ Verifice securitatea configurațiilor, în conformitate cu stadiul tehnicii, cerințele minime de asigurare a securității rețelelor și sistemelor informatice și regulile specifice ale OE, respectiv a:
  - ➢ echipamentelor de rețea cu fir sau fără fir (cum ar fi switch-uri sau routere);
  - ➢ echipamentelor de securitate (tip firewall sau releu invers, filtrare sau nu, și regulile lor de filtrare, criptare etc.);
  - ➢ sistemelor de operare;
  - ➢ sistemelor de gestionare a bazelor de date;
  - ➢ serviciilor de infrastructură;
  - ➢ serverelor de aplicații;
  - ➢ stațiilor de lucru;
  - ➢ echipamentelor de telefonie;
  - ➢ mediilor de virtualizare.

Pentru a solicita cat mai clar servicii de audit

- Definiti cerintele: Identificati sistemele si serviciile critice care trebuie auditate si specificati cerintele si obiectivele auditului.
- Cautati furnizori potriviti: Cautati furnizori de servicii de audit NIS atestati de catre DNSC, care au experienta si expertiza necesare pentru a indeplini cerintele dumneavoastra. Lista furnizorilor o gasiti pe site-ul DNSC.
- Solicitati oferte: Contactati furnizorii selectati si solicitati oferte detaliate care sa cuprinda informatii despre metodologia lor, personalul implicat, costurile si termenele de livrare.
- Evaluati ofertele: Evaluati ofertele primite si comparati-le in functie de costuri, calitatea serviciilor si abilitatea furnizorilor de a indeplini cerintele dvs.
- Negociati: Discutati cu furnizorii selectati si negociati termenii si conditiile contractului, cum ar fi costurile, perioada de audit si responsabilitatile partilor
- Semnati contractul: Semnati contractul cu furnizorul ales si asigurati-va ca acesta reflecta in mod clar termenii si conditiile convenite
- Monitorizati: Monitorizati progresul auditului si colaborati cu furnizorul pentru a rezolva orice probleme sau a clarifica orice intrebari.