QEVERISJA DHE STANDARDET E SIGURISË KIBERNETIKE

Governance, Risk, and Compliance – Qeverisje, Menaxhim i Rrezikut dhe Përputhshmëria

Përbërësit kryesorë të GRC-së:

- *Qeverisja*
- *Strategjia*
- *Menaxhimi i Rrezikut*
- *Përputhshmëria*
- *Promovimi*

Ligjet, Rregulloret dhe Metodologjitë në RSH

- **Ligji per Sigurinë Kibernetike 25/2024**
- Rregullore mbi **Mënyrën e Dokumentimit dhe Implementimit të Masave** të Sigurisë në Infrastrukturat Kritike dhe të Rëndësishme të Informacionit
- Metodologjisë për Vlerësimin dhe Analizimin e **Rrezikut** të Sigurisë Kibernetike
- Rregullore për **Kategorizimin e Incidenteve** të Sigurisë Kibernetike
- Procedurat e **Menaxhimit të Incidenteve** të Sigurisë Kibernetike, Kundërmasat, Playbooks dhe Masat Mbrojtëse të Natyrës së Përgjithshme
- Rregullore për **Funksionimin Teknik të CSIRT-ve** Sektoriale dhe CSIRT-eve pranë Operatorëve të Infrastrukturave të Informacionit

Rregullorja e Masave - V3.0 05.03.2024

Qëllimi i Rregullores

Objektivat dhe Strukturimi

- Organizative
- Teknike

Niveli Sigurise

- 1 – masa te uleta dhe te mesme OIKI &OIRI
- 2 – masa te avancuara OIKI

Dokumentimi dhe Verifikimi

- Politika/Procedura
- Raportet teknike
- Evidenca

ISO 27001

ISO 27001 është një ***standard ndërkombëtar*** *që përcakton kërkesat për krijimin, zbatimin, mirëmbajtjen dhe përmirësimin e vazhdueshëm të një* ***Sistemi të Menaxhimit të Sigurisë së Informacionit (ISMS)***.

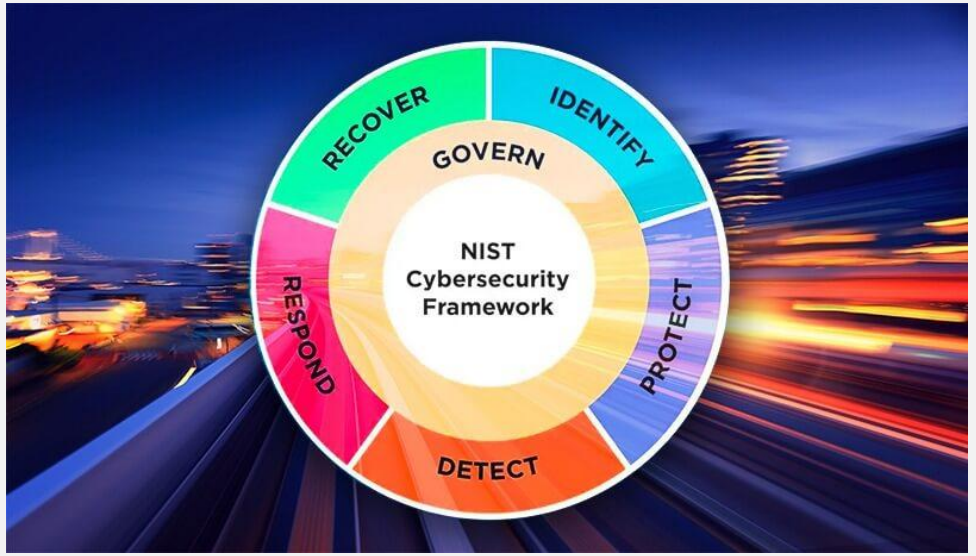
Rëndësia e ISO 27001 per infrastrukturën kritike:

- Mbrojtja e të Dhënave të Ndjeshme
- Vazhdimësia e Operacioneve
- Menaxhim Proaktiv i Rreziqeve
- Përputhshmëri Ligjore
- Besimi i Palëve të Interesuara
- Ndërgjegjësimi dhe Trajnimi i Punonjësve:

NIST CSF

5 Funksionet Kryesore

1. IDENTIFIKO
2. MBRO
3. ZBULO
4. PERGJIGJU
5. RIMEKEMB

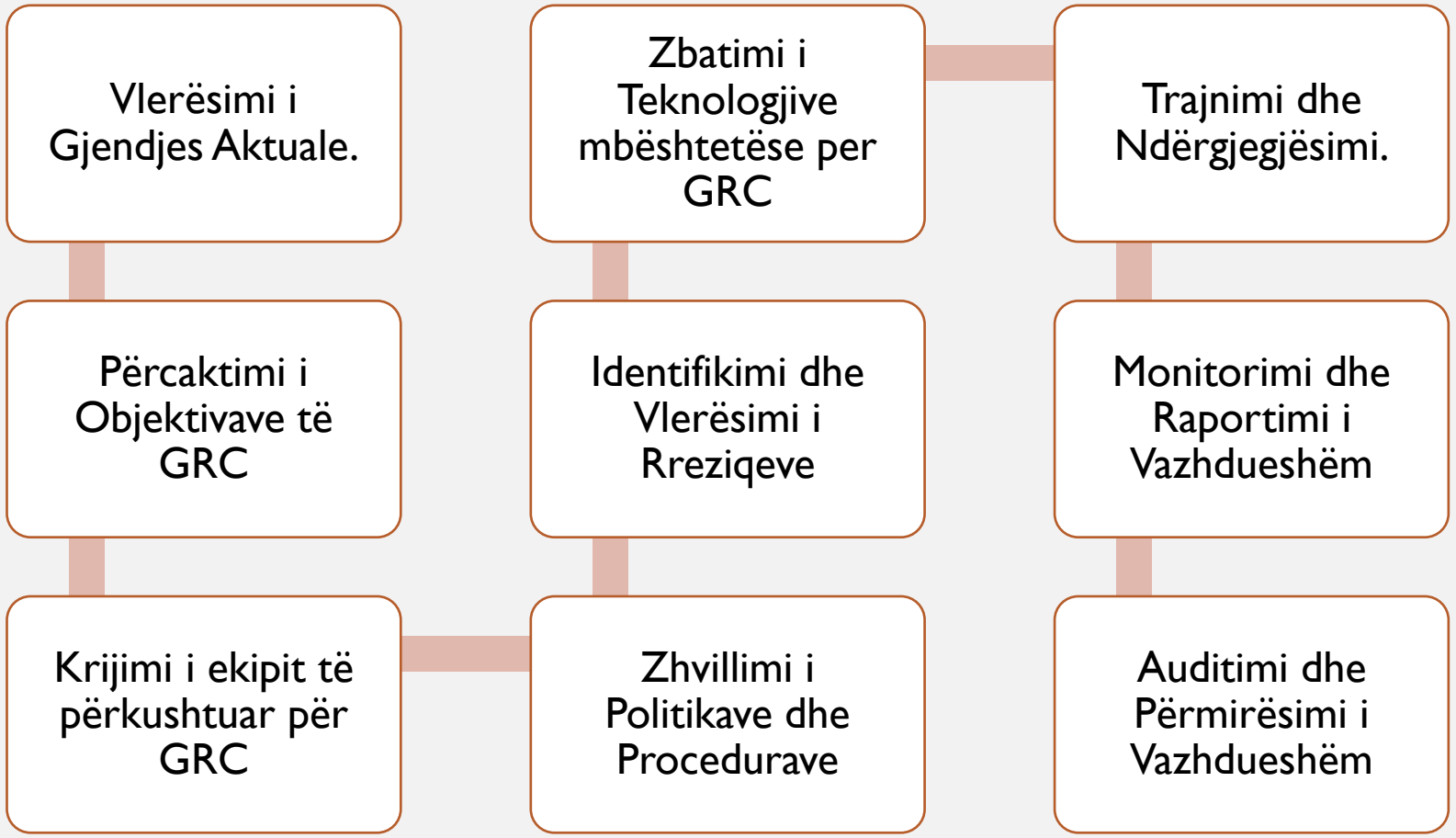


DIREKTIVA NIS2

Kërkesat për Organizatat

- Menaxhimi i rrezikut
- Raportimi i detyrueshëm i incidenteve
- Siguria në zinxhirin e furnizimit
- Masat Teknike dhe Organizative
- Auditime dhe Testime të Rregullta
- Përgjegjësia e Menaxhmentit
- Ndarja e Informacionit dhe Bashkëpunimi

HAPAT KRYESORË PËR IMPLEMENTIMIN EFEKTIV TË GRC



SHEMBULL: ZBATIMI I GRC NË U.K “UJË I PASTËR 21”

Rreth Organizatës

- Ndërmarrje publike e ujësjellës-kanalizimeve
- Shërben mbi 100,000 banorë
- Sisteme të digjitalizuara: SCADA, faturim, rrjet IT

Pse i duhet GRC-ja?

- Rritje e rreziqeve kibernetike
- Kërkesa për përputhshmëri me ligjin dhe rregulloren e masave
- Nevoja për qeverisje dhe kontroll më të mirë

IMPLEMENTIMI GRC TEK “UJË I PASTËR 21”

1. Vlerësimi Fillestar
- Analizë e sistemeve SCADA dhe IT
- Identifikim boshllëqesh në PPT

2. Përcaktimi i Objektivave
- Siguri për sistemet kritike
- Përputhshmëri me ligjet dhe rregulloret
- Menaxhim i rrezikut

3. Krijimi i Ekipit GRC
- IT, juridik, teknik, auditim
- Mbështetje nga drejtori i përgjithshëm

4. Politika dhe Procedura
- Akses në SCADA
- Menaxhim incidentesh
- Mbrojtje të dhënash të konsumatorëve

5. Teknologjia GRC
- Platformë e thjeshtuar GRC
- Integrim me sistemet ekzistuese

6. Trajnimi i Stafit
- Ndërgjegjësim për sigurinë
- Raportim incidentesh

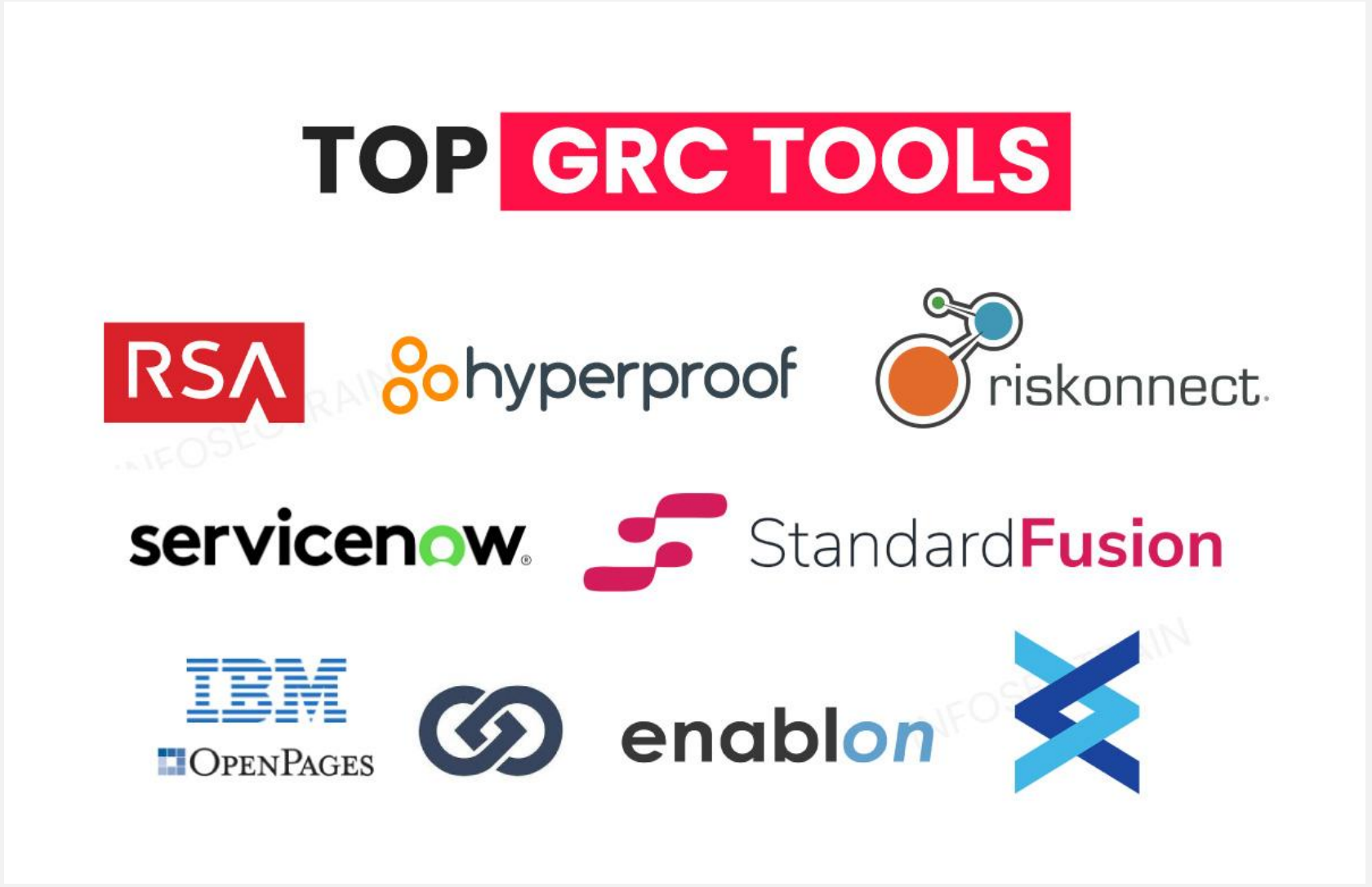
7. Monitorim & Raportim
- KPI për përputhshmëri dhe reagim
- Raporte për drejtuesit

8. Auditim & Përmirësim
- Auditim i brendshëm pas 6 muajsh
- Përmirësim i kontrollit të aksesit fizik

MJETET DHE TEKNOLOGJITË GRC

- Menaxhim i centralizuar i rrezikut
- Perputhshmëri me rregullore dhe standarde
- Auditim dhe gjurmueshmëri
- Reagim më i shpejtë ndaj incidenteve
- Vendimmarrje e bazuar në të dhëna
- Menaxhim i palëve të treta (third-party risk)
- Automatizim dhe efikasitet

MJETET (TOOLS) MË TË NJOHURA PËR GRC



MENAXHIMI INCIDENTIT KIBERNETIK

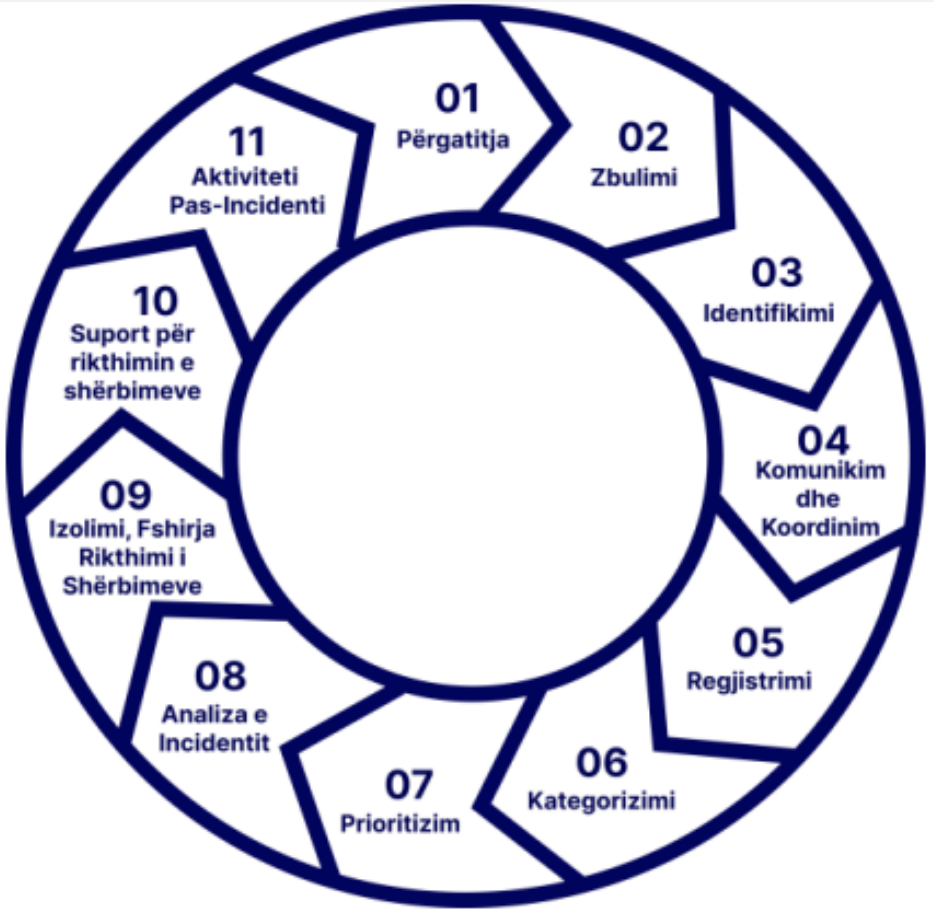


Figura 1: Cikli i Menaxhimit të Incidentit Kibernetik

SFIDAT DHE TENDENCAT E GRC-SË

🔴 **Sfidat Kryesore:**

• ***Rritja e kompleksitetit*** të rregulloreve dhe standardeve ndërkombëtare

• ***Mungesa e vizibilitetit në kohë reale*** mbi rreziqet kibernetike

• ***Integrimi i dobët*** midis GRC dhe sistemeve të sigurisë ekzistuese

• ***Menaxhimi i rrezikut nga palët e 3ta***

• ***Burime të kufizuara*** për pajtueshmëri dhe auditim

🟢 **Tendencat Aktuale:**

• ***Automatizimi i kontrollit*** dhe mbledhjes së provave (Continuous Controls Monitoring)

• ***Integrimi i GRC me ITSM dhe SecOps*** për reagim më të shpejtë

• ***Përdorimi i inteligjencës artificiale*** për analizën e rrezikut, IoC-ve, VA, etj.

• ***Platforma të centralizuara*** për menaxhimin e rrezikut dhe pajtueshmërisë

• ***Fokus i shtuar në privatësinë*** e të dhënave dhe rrezikun e palëve të 3ta

FALEMINDERIT!

- https://aksk.gov.al/
- https://www.facebook.com/aksk.gov.al
- https://www.instagram.com/aksk.gov.al/
- https://www.linkedin.com/company/aksk-gov-al/