

# **QEVERISJA DHE STANDARDET E SIGURISË KIBERNETIKE**

**Zbatimi në Infrastrukturën Kritike  
dhe të Rëndësishme të Informacionit**



# Kuadri i Qeverisjes, Rrezikut dhe Pajtueshmërisë (GRC) dhe Praktikrat më të Mira

**Implementimi në Infrastrukturën Kritike**



# Çfarë është GRC?



**Përkufizimi i GRC:** Një qasje gjithëpërfshirëse dhe e integruar për menaxhimin e qeverisjes, rrezikut dhe aktiviteteve të pajtueshmërisë së një organizate.

## **Elementët Kryesore:**

- **Qeverisja:** Krijimi i politikave, proceseve dhe përgjegjësi dhe roleve të qarta për vendimmarrje.
- **Strategjia:** Zhvillimi dhe implementimi i një strategjie kibernetike
- **Menaxhimi i Rrezikut:** Identifikimi, vlerësimi, prioritizimi dhe zbutja e rreziqeve të mundshme.
- **Pajtueshmëria:** Sigurimi i respektimit të ligjeve, rregulloreve dhe standardeve të industrisë në fuqi.
- **Promovimi :** Krijimi i një kulture gjithëpërfshirëse për sigurinë kibernetike dhe standartin e zbatuar.

# ISO 27001: Standard për Sigurinë e Informacionit

Një standard i njohur globalisht që përshkruan praktikat më të mira për krijimin, zbatimin, mirëmbajtjen dhe përmirësimin e vazhdueshëm të një sistemi të menaxhimit të sigurisë së informacionit (ISMS).

## Komponentët Kryesorë:

Vlerësimi dhe menaxhimi i rrezikut

Zhvillimi dhe zbatimi i politikave

Trajnimi për kontrollin e aksesit dhe ndërgjegjësimin e sigurisë

Menaxhimi dhe reagimi i incidentit

# Korniza e Sigurisë Kibernetike NIST:

Përmbledhje e Kornizës së Sigurisë Kibernetike NIST: Një kornizë vullnetare që ofron një sërë praktikash dhe udhëzimesh më të mira për menaxhimin e rreziqeve të sigurisë kibernetike.



# Direktiva NIS2:

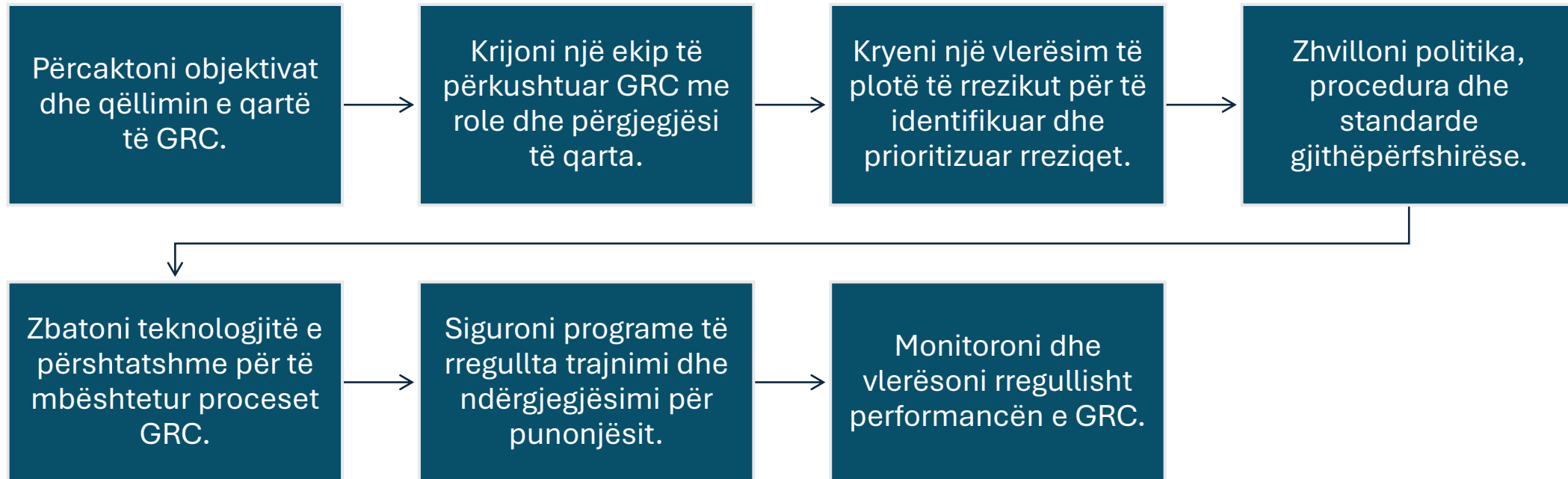
Pasqyrë e Direktivës NIS2: Një rregullore e Bashkimit Evropian që synon forcimin e sigurisë kibernetike për entitetet thelbësore nëpër sektorë kritikë.

## Kërkesat Kryesore:

- Vlerësimi i rrezikut dhe detyrimet e raportimit të incidenteve.
- Masat e shtuara të sigurisë për sistemet dhe rrjetet e informacionit.
- Bashkëpunimi dhe shkëmbimi i informacionit ndërmjet palëve të interesuara.



# Hapat Kryesorë për Zbatimin Efektiv të GRC:



# GRC: Një Element Thelbësor për Sigurimin e Infrastrukturës Kritike



## Rëndësia e GRC në Infrastrukturën Kritike:

Ruajtja e vazhdimësisë dhe elasticitetit operacional

Mbrojtja e aseteve kritike dhe informacionit të ndjeshëm

Sigurimi i pajtueshmërisë me rregulloret dhe standardet përkatëse

Zbutja e rreziqeve për sigurinë publike dhe sigurinë kombëtare



# Mjetet dhe Teknologjitë GRC

Kompleksiteti i natyrshëm i menaxhimit të GRC kërkon përdorimin e mjeteve dhe teknologjive të specializuara.

GRC tools, ndihmojnë organizatat në automatizimin dhe thjeshtimin e aktiviteteve të tyre, duke identifikuar, vlerësuar dhe zbutur rreziqet në mënyrë efektive.

Ato përmirësojnë monitorimin dhe raportimin e përputhshmërisë, duke ofruar një perspektivë të integruar mbi gjendjen e përgjithshme të organizatës.

# Disa nga mjetet (tools) më të njohura për GRC:

- RSA Archer
- IBM OpenPages
- MetricStream
- ServiceNow GRC
- NAVEX Global
- SAP GRC
- LogicGate

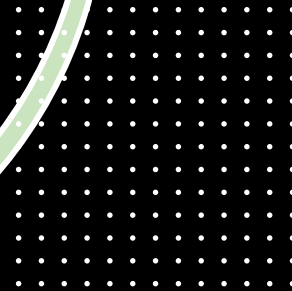


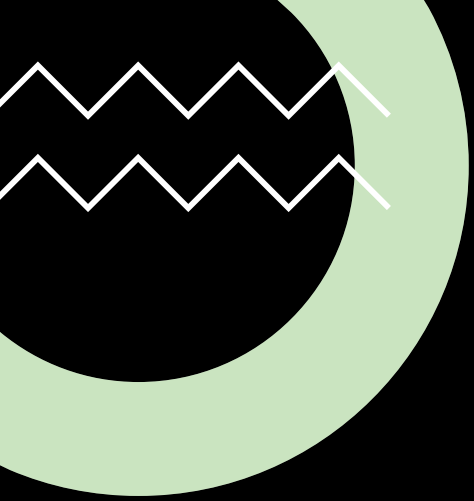


# Rast Studimi: Kompania Supozuar CyberGuard

## CyberGuard: Zbatimi i një Kuadri të Suksesshëm GRC

- Pasqyrë e organizatës dhe infrastrukturës së saj kritike.
- Sfidat kryesore me të cilat përballet organizata në lidhje me GRC.
- Strategjitë e zbatuara për të rritur aftësitë e GRC.
- Rezultatet e matshme dhe ndikimi i zbatimit të GRC.





# Detaje mbi Komponentët e GRC



# Qeverisja: Vendorsja e Themelit për GRC

- Vendorsja e roleve dhe përgjegjësi të qarta për aktivitetet e GRC.
- Përcaktimi i strukturave qeverisëse, komiteteve dhe linjave të raportimit.
- Sigurimi i mbikëqyrjes dhe llogaridhënies efektive për performancën e GRC.

*Shembuj të Strukturave Qeverisëse në Infrastrukturën Kritike:*

- *Bordet e Drejtorëve*
- *Komitetet e Menaxhimit*
- *Grupet e Mbikëqyrjes së Sigurisë*

# Menaxhimi i Rrezikut: Identifikimi dhe Zbutja e Kërcënimeve

---

Kryerja e vlerësimeve gjithëpërfshirëse të rrezikut për të identifikuar kërcënimet dhe dobësitë e mundshme.

---

Prioritizimi i rreziqeve bazuar në gjasat dhe ndikimin.

---

Zhvillimi i strategjive për zbutjen e rrezikut dhe zbatimi i kontrolleve.

---

Shembuj të Teknikave të Menaxhimit të Rrezikut në Infrastrukturën Kritike:

Modelimi i Kërcënimit

Skanimi i Cenueshmërisë

Testimi i Penetrimit



# Pajtueshmëria: Sigurimi i Respektimit të Rregullave ndaj Rregullatorëve

Kuptimi i ligjeve, rregulloreve dhe standardeve të industrisë në fuqi që lidhen me infrastrukturën kritike.

Zbatimi i politikave dhe procedurave për të siguruar pajtueshmërinë.

Kryerja e auditimeve dhe vlerësimeve të rregullta të pajtueshmërisë.

*Shembuj të Kërkesave të Pajtueshmërisë për Infrastrukturën Kritike:*

- *Rregulloret e Sigurisë Kibernetike*
- *Ligjet për Privatësinë e të Dhënave*
- *Standardet Specifike të Industrisë*



# Zhvillimi i Politikave: Vendosja e Rregullave të Lojës

-Zhvillimi i politikave, procedurave dhe standardeve gjithëpërfshirëse të GRC.

-Sigurimi që politikat janë të qarta, koncize dhe të arritshme për të gjithë punonjësit.

-Komunikimi i politikave në mënyrë efektive përmes programeve të trajnimit dhe ndërgjegjësimit.

*Shembuj të Politikave Kryesore të GRC për Infrastrukturën Kritike:*

- *Politika e Sigurisë së Informacionit*
- *Politika e Reagimit ndaj Incidenteve*
- *Politika e Përdorimit të Pranueshëm*





# Teknologjia: Rritja e Efikasitetit dhe Efektivitetit të GRC

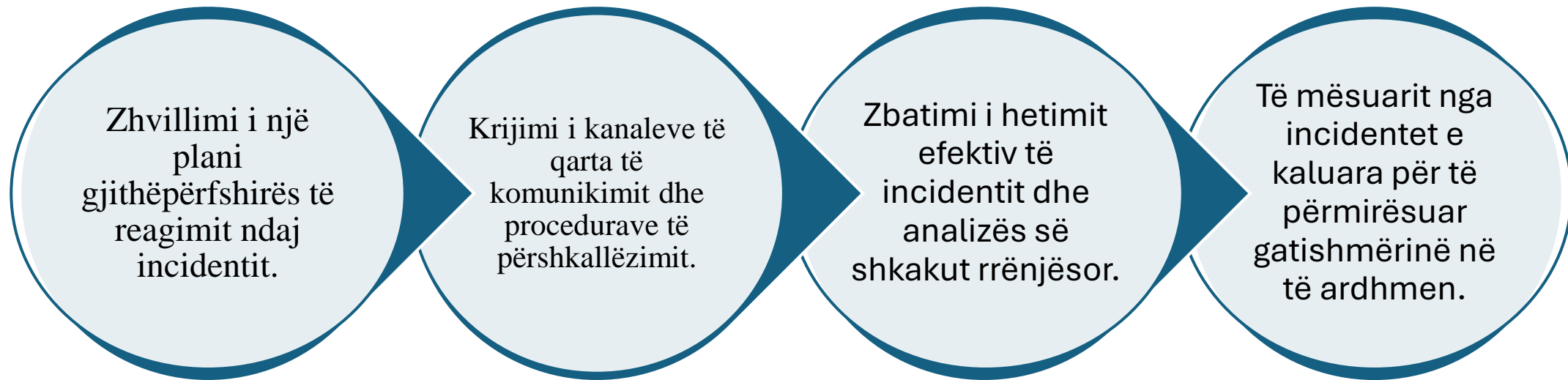
Përdorimi i teknologjisë për të automatizuar dhe thjeshtuar proceset GRC.

Zbatimi i zgjidhjeve softuerike të GRC për vlerësimin e rrezikut, ndjekjen e pajtueshmërisë dhe menaxhimin e incidenteve.

*Shembuj të Teknologjive GRC:*

- *Platformat e Menaxhimit të Rrezikut*
- *Sistemet e Menaxhimit të Pajtueshmërisë*
- *Skansuesit e Cenueshmërisë*

# Menaxhimi i Incidentit: Përgjegjja ndaj Ndërprerjeve dhe Mësimi nga Përvoja



# Ndërgjegjësimi për Sigurinë:





## Përmirësimi i Vazhdueshëm:

- Vlerësimi i rregullt i efektivitetit të proceseve të GRC.
- Kryerja e auditimeve dhe vlerësimeve periodike për të identifikuar fushat për përmirësim.
- Përshtatja e proceseve GRC ndaj kërcënimeve, teknologjive dhe rregulloreve në zhvillim.



# E Ardhmja e GRC në Infrastruktura

## Tendencat në Zhvillim në GRC:

- Inteligjenca Artificiale (AI) dhe Mësimi i Makinerive për Parashikimin dhe Automatizimin e Rrezikut.
- Teknologji Blockchain për Ndarje të Sigurt të të Dhënave dhe Gjurmueshmëri.
- Cloud Computing për Shkallëzim dhe Fleksibilitet të Zgjerruar.

## Sfidat me të Cilat Përballet GRC në Infrastrukturën Kritike:

- Kërcënimet Kibernetike Gjithnjë e më të Sofistikuara.
- Teknologjitë dhe Rregulloret me Zhvillim të Shpejtë.
- Mungesa e Profesionistëve të Aftë të Sigurisë Kibernetike.

# GRC: Një Fondacion për një të Ardhme të Sigurt dhe Elastike



- GRC është thelbësore për ruajtjen e infrastrukturës kritike.
- Kornizat efektive të GRC-së kërkojnë një qasje gjithëpërfshirëse dhe angazhim të vazhdueshëm.
- Zbatimi i praktikave më të mira të GRC-së çon në përmirësimin e menaxhimit të rrezikut, pajtueshmërisë dhe qëndrueshmërisë operacionale.
- E ardhmja e GRC përfshin përqafimin e teknologjive në zhvillim dhe përshtatjen ndaj kërcënimeve në zhvillim.





# Faleminderit

