

# Leveraging AI for DORA compliance assessment in insurance



Eivind Borg  
eivind@analytika.no  
+47 99 21 67 98

# Can we combine AI and compliance?



+



=

?

Challenges



**ANALYTIKA**

Our Solution: combine AI and human expertise



# Example result

(“ICT-related incident management, classification and reporting”)

## INPUT:

### Incident Management Policy

#### Scope

*This policy applies to all ICT-related incidents that have an adverse impact on the availability, authenticity, integrity, or confidentiality of data, or on the services provided by the organization.*

.....

## EXAMPLE OUTPUT:

**requirement:** *Article 17 paragraph 3*

**compliant:** *Compliant.compliant*

**explanation:** *The policy is compliant with the requirements of Article 17 paragraph 3. It establishes early warning indicators and procedures to identify, track, log, categorize and classify ICT-related incidents according to their priority and severity. It assigns roles and responsibilities for different ICT-related incident types and scenarios. It sets out plans for communication to staff, external stakeholders and media, and for notification to clients. It ensures that at least major ICT-related incidents are reported to relevant senior management and informs the management body of such incidents, explaining the impact, response and additional controls to be established. It also establishes ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner.*

**requirement:** *Article 18 paragraph 1*

**compliant:** *Compliant.partially\_compliant*

**explanation:** *The policy does classify incidents according to their severity and impact, which is in line with the requirement. However, the policy does not explicitly state that the classification and determination of impact is based on the specific criteria outlined in the requirement, such as the number and relevance of clients affected, the duration of the incident, the geographical spread, data losses, the criticality of the services affected, and the economic impact. Therefore, the policy is only partially compliant with the requirement.*

**requirement:** *Article 18 paragraph 2*

**compliant:** *Compliant.not\_compliant*

**explanation:** *The policy does not provide a classification of cyber threats based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk. The policy only classifies incidents according to their severity and impact, but does not take into account the specific factors mentioned in the requirement.*





Going forward



Eivind Borg  
eivind@analytika.no



**ANALYTIKA**

<https://www.analytika.no>