Dear,

In the new draft I do not find any clear integration from the notification process (incidents, suspicious activities, abnormal movements…) to federal instances, incident response teams, security forums....
US and EU regulations are evolving and make already higher assumptions. For instance, laws about privacy, anti-money laundering, anti-terrorism… require that any cybersecurity framework incorporates the proper notification process in its core.
In current draft, the suspicious activities management is mainly part of the ID, DE & RS layers.
Wouldn't it be interesting to add a section / (transversal or additional) layer dedicated to it?

Regards