

FIMI monitoring templates

CHECKLIST



FDEI
PROJECT

FIMI
-ISAC

This document provides a concise, easy-to-use checklist that helps users apply the three FIMI monitoring templates – 1. Incident qualification, 2. (Systemic) violations, and 3. Counter-measures – quickly and efficiently.

Checklist for incident qualification (PART 1)

A. IS THIS FIMI?		
1. FOREIGN ACTORS		
Are foreign actors engaging in this incident/campaign?*	Yes	No
If yes, are they state or non-state actors ?	Yes	No
If yes, are they the initiators ?	Yes	No
If yes, are they the amplifiers ?	Yes	No
If amplifiers, is there evidence of a direct connection with the initiators?*	Yes	No
<i>*If the answer is no, then the incident/campaign is <u>NOT</u> FIMI.</i>		
2. BEHAVIOUR		
2.1 MANIPULATION		
Does the incident/campaign show manipulative behaviour?	Yes	No
If yes, does it include disinformation ?	Yes	No
If yes, what is the narrative circulated?	Describe	
Did a cyberattack happen before or after the (dis)information was shared?	Yes	No
Does the incident/campaign use other TTPs for manipulative purposes?	Yes	No
2.2 INTENTIONALITY		
Does the incident/campaign show evidence of intentionality ?	Yes	No
Is the purpose of the incident/campaign clear?	Yes	No
2.3 COORDINATION		
Does the incident/campaign show evidence of coordination ?	Yes	No
3. IMPACT		
Did the incident/campaign achieve considerable outreach ?**	Yes	No
Did the incident/campaign achieve considerable engagement ?**	Yes	No

Does the incident/campaign harm/criticise/attack the core values of EU societies?	Yes	No
Does the incident/campaign harm/criticise/attack the core procedures of EU societies?	Yes	No
<i>**Define concepts of outreach and engagement explicitly and set a threshold within the working group or project</i>		
4. INFRINGEMENT***		
Does the incident/campaign constitute a law violation ?	Yes	No
If yes, does it violate national regulations ?	Yes	No
If yes, does it violate international regulations ?	Yes	No
If not, does it constitute a harmful activity?	Yes	No
If not, does it violate the platform's Terms of Service ?	Yes	No
<i>***No prior legal background is needed. Where helpful, desk research and analytical support tools may be cautiously used to guide the process, always cross-checking and validating outputs against reliable sources.</i>		
FINAL ASSESSMENT		
<ul style="list-style-type: none"> ● Low certainty: There is no evidence that the incident is part of a FIMI operation. ● Medium certainty: Several of the conditions are met and supported by evidence. The investigator strongly believes the incident is FIMI, but there is not enough evidence to confirm it. ● High certainty: All conditions are met and backed by evidence. The investigator can confidentially confirm the incident is part of a FIMI operation. 		
B. SINGLE INCIDENT OF PART OF A CAMPAIGN?		
Does the incident/campaign show evidence of coordination?	Yes	No
Does the single incident show evidence of coordination among foreign actors? If yes, this is a FIMI incident	Yes	No
Do multiple incidents show evidence of coordination among each other? If yes, this is a FIMI campaign	Yes	No
FINAL ASSESSMENT:		
<ul style="list-style-type: none"> ● Single incident: There is currently no evidence that the incident is part of a broader FIMI campaign. ● Part of a campaign: One coordinated incident or multiple incidents indicate that the activity is part of an ongoing FIMI campaign. 		

Checklist for (systemic) violations (PART 2)

Disclaimer: Using this checklist does not require any prior legal background. Where helpful, desk research and analytical support tools may be used to guide the process. However, such tools should be used cautiously, and outputs should be cross-checked and validated against reliable sources.

Shorter version:

→ Use this checklist for a quick assessment of potential (systemic) infringements

Incident ID	When was the incident created and registered ? Ideally, record reports for each platform separately	Describe	
Assessing the violation	Does the incident/campaign constitute a violation ? + Describe	Yes	No
Assessing the type of violation	If yes, is it a violation of national or international/EU law ? + Describe	Yes	No
	If yes, is it a violation of the platform's Terms of Service ? + Describe	Yes	No
Assessing systematicity [inaction]	Are you aware of platform inaction regarding the incident? + Describe	Yes	No
Assessing systematicity [inconsistency]	Are you aware of platform inconsistency regarding the incident? + Describe	Yes	No
Assessing systematicity [recurrence]	Are you aware of the same/a similar incident occurring on the platform? + Describe	Yes	No

Extended version:

→ Use this extended checklist for a more thorough assessment of potential (systemic) infringements

A. INCIDENT ID		
Record incident creation date and incident registration date Ideally, record reports for each platform separately		
B. TYPE OF INFRINGEMENT		
Record any element that is already under investigation for a possible DSA violation (e.g., misuse of verified accounts, lack of transparency in political ads, manipulation of recommender systems)		
Do you suspect that the incident may constitute an infringement ?		Yes No

If the incident is content-related, is the content harmful ?	Yes	No
If the incident is content-related, is the content illegal ?	Yes	No
If illegal, does the incident/campaign's content violate national legislation ?	Yes	No
If illegal, does the incident/campaign's content violate international legislation ?	Yes	No
If illegal, does the incident/campaign's content violate a platform's Terms of Service ?	Yes	No
If the incident is behaviour/TTP-related, is the behaviour/TTP harmful ?	Yes	No
If the incident is behaviour/TTP-related, is the behaviour/TTP illegal ?	Yes	No
Does the incident/campaign's behaviour/TTP violate national legislation ?	Yes	No
Does the incident/campaign's behaviour/TTP violate international legislation ?	Yes	No
Does the incident/campaign's behaviour/TTP violate a platform's Terms of Service ?	Yes	No
If there is a violation of national law (e.g., impersonation, hate speech, incitement to violence, etc.) or international law (e.g., DSA, AI Act, GDPR, etc.), describe it, try to identify the legal ground , and identity who is accountable for it	Describe	
Is there a violation of a platform's Terms of Service (e.g., scam ads, fake accounts, bots etc.), describe it and try to identify the contractual ground (e.g., authenticity, coordinated inauthentic behaviour, ad standards, etc.)	Yes	No
C. SYSTEMIC INFRINGEMENT		
1. PLATFORM (IN)ACTION		
Has the incident been reported/flagged ?	Yes	No
If yes, did the researcher (or someone known) report/flag the incident publicly ?	Yes	No
If yes, did the researcher (or someone known) report/flag through platform reporting mechanisms ?	Yes	No
If yes, did the platform take any action against the incident?	Yes	No
If yes, what action did the platform take (e.g., label, downrank, remove, etc.)?	Describe	
If yes, when did the platform take action?	Describe	
2. REPETITION/RECURRENCE		
Is the researcher aware of the same/a similar incident that happened before ?	Yes	No

If yes, with what occurrence ?	Describe	
If yes, was it already known to the platform as a misuse/risk?	Yes	No
Did the platform respond consistently across all cases?	Yes	No
Did the platform take no action in any case?	Yes	No
Did the platform take action in some cases but not in others?	Yes	No
Did the platform take the same action in all cases?	Yes	No
Did the platform take different actions in different cases?	Yes	No
Did the platform implement any measures to prevent similar incidents from happening again?	Yes	No
If yes, what measures ?	Describe	
If yes, did they prove effective in reducing recurrence of the incident(s)?	Yes	No
FINAL ASSESSMENT		
Is there evidence that the infringement was caused by the design or functioning of the platform?	Yes	No
Is the infringement a DSA violation ?	Yes	No

Checklist for countermeasures (PART 3)

A. COUNTERMEASURES IN PLACE		
1. STAKEHOLDERS INVOLVED		
Who has taken action (e.g., researchers, platform, victims, etc.)	Describe	
2. ACTION TAKEN		
Were they exposure -related countermeasures? + Describe	Yes	No
Were they community engagement -related countermeasures? + Describe	Yes	No
Were they distribution -related countermeasures? + Describe	Yes	No
Were they infrastructure -related countermeasures? + Describe	Yes	No
Were they sanctions and legal -related countermeasures? + Describe	Yes	No
Were they media literacy -related countermeasures? + Describe	Yes	No
3. IMPACT	Yes	No
Did the countermeasures raise awareness of the incident? + Describe	Yes	No
Did they impact the threat actor capabilities to produce/distribute disinformation? + Describe	Yes	No
Did they trigger other actions by the defender community or threat actor(s)? + Describe	Yes	No
Did they reinforce the attribution of the incident? + Describe	Yes	No
Did they deter the threat actor(s)? + Describe	Yes	No

4. LEGAL GROUNDS		
Are the countermeasures based on national law, international law, or platform Terms of Service? + Describe	Yes	No
B. POTENTIAL ADDITIONAL COUNTERMEASURES		
Is there anything more that could be done to stop/mitigate the incident?	Describe	

A large blue circle containing the text "EU DISINFO LAB" in white. The word "LAB" is enclosed in a white speech bubble shape. A black line extends from the top-left of the circle towards the center of the page.

EU DISINFO LAB

This template was created as part of EU DisinfoLab's contributions to the [FIMI-ISAC FIMI Defenders For Election Integrity \(FDEI\) project](#), an initiative that brought together 10 European organisations to collaboratively detect and respond to FIMI in electoral processes. The project aims to bolster democratic institutions by providing tools, establishing response teams, and creating an operational handbook.

A dark blue circle containing the logo for the FDEI Project. The logo consists of a stylized 'F' made of three vertical bars of increasing height, followed by the text "FDEI" in a large, bold, sans-serif font, and "PROJECT" in a smaller font below it.

FDEI
PROJECT

A black circle containing the logo for FIMI-ISAC. The logo features a stylized graphic of three overlapping circles on the left, followed by the text "FIMI" in a large, bold, sans-serif font, and "-ISAC" in a smaller font below it.

FIMI
-ISAC