

Convention on the Manipulation of Sports Competitions Group of Copenhagen – Alert System Handbook on Alert and Surveillance system



(version 5 December 2017)

1. Introduction:

In order to achieve efficient and fast reactions in the fight against match fixing, the French NP proposed three different tools during the 3rd GoC meeting in Paris (March 2016). The GoC has decided to test those tools. The Danish NP has been designated as secretariat to this working group and at the same time work on the preparation of Action Cards, relevant templates and suggestions to improved communication between relevant stakeholders.

The use of these tools will ensure a common base-line of understanding and a corresponding alignment of communication and work procedures. Action Cards and templates should be viewed as a set of overall guidelines that can ensure the operational partners a common “language”, based on good practices.

Overall, we have chosen to categorize *four basic levels of alerts*. There are *four analogue alarm levels* connected to these. Briefly, the level of alert describes internal work procedures, whereas the alarm level is the way stakeholders inform and communicate with other external relevant partners.

The classification of levels starts from "normal" and can rise to the "highest level". This division seeks to ensure a reasonable framework to differentiate between different types of event or scenario. It is up to the individual case manager, based on thorough validation of the available data, to choose an appropriate level of alert. For each level, the Action Card will have a number of recommendations for procedures that should be observed.

As mentioned above, it is proposed that there will be an "alarm level" connected to every "alert level". The working group has attempted to design a useful, easily accessible template to support this process. Thus, when receiving a letter of alert from a given partner, there will be an expectation that the recipient initiates the appropriate measures in relation to the content of the transmitted information.

Finally, in this memorandum, recommendations for procedures concerning secure and encrypted communication between stakeholders are also discussed, and we present a methodology for this as well.

2. Description of alert and notification levels and presentation of Action Card text:

The Action Card: Notice Levels connects the four alert levels to a unique color code. This color code will resume on the alert template and allows recipients to quickly visually determine the nature of the alerted event. Combination of color and category is shown below:

- Green (Normal)
- Yellow (Slightly increased alert)
- Orange (Increased alert)
- Red (Highest alert)

Green:

Green (Normal): This level can best be described as the "normal" level. There are no indications from either internal or external sources that indicate match fixing or other irregularities.

Green Alert: Communication should only be sent out when an *increased* alert level is settled and *returns* to alert level Green. The communicated message should always contain a preliminary conclusion, as well as a reason for choosing to return to the norm.



Green Alarm: Receiving a Green Alert means in practice that the sender no longer finds reason to be at a higher alert level. The recipient may return to normal daily operations.

Below the Action Card text is shown:

Level:	Description:	Suggested procedures for National Platform:
Green	No indications from: <ul style="list-style-type: none"> • Stakeholders • OSINT (Open Source Intelligence) • Media 	Return to normal procedures

Yellow:

Yellow: (Slightly increased alert): The result of several different indications of irregularities. For example, there may be unexplained fluctuations in odds, rumors on social media or source information, but the intelligence can not immediately be validated as credible or probable.

Different organizations usually work at this level a large part of the time solving their daily tasks. Therefore, it is not to be expected that all platform stakeholders will be alerted about events of this nature. A more-detailed review of the incident will often explain the cause and procedures will return to "normal". It is useful to save documentation regarding the event, such as people associated with the incident, bets placed, etc. This information may later be of importance in another context.

Yellow Alert: Communication can be used as a notification to relevant partners. It can also be used as a request in different respects. The yellow alert requires a number of additional measures compared to normal procedure (see Action Card). A yellow alert will therefore most often be shared between specific stakeholders chosen by the sender.

Yellow Alarm: Receiving a yellow alert will often mean the implementation of a number of appropriate measures, including the collection of specific requested information or involve further distribution of the information, etc.

Below the Action Card text is shown:

Level:	Description:	Suggested procedures for National Platform:
Yellow	Indications from: <ul style="list-style-type: none"> • Irregular betting patterns / odds movements Unverified information from e.g.: <ul style="list-style-type: none"> • Social Media • Chat forum • Secondhand accounts 	<ul style="list-style-type: none"> • Collection and documentation of information. • Contact to specific stakeholders • Documentation of conclusion - return to normal level with Green Notice. • Send Green Notice including immediate conclusion. • Submit notification to "Sharefile Logbook" (ARJEL) • logbook@arjel.fr

Orange:

Orange: (Increased alert): This level is used when, after careful assessment / validation, it seems likely that match fixing is probable or imminent, however, without finding concrete evidence for this. The assessment should be based on several sources, but may in special cases also be based on information from a single source. These could include: A sustained unexplained development in the betting market, a credible whistleblower or similar. However, it is important to point out that the fewer sources that support a concrete assessment, the greater the requirement for the credibility of the source.

Orange Alert: Sending an orange alert may contain a specific suspicion, the basis for this or direct information about the fixing itself - but it can also be used as a query for any missing information that can prove that fixing is taking place. An orange alert is expected to be communicated to a wide range of national and international stakeholders, including other National Platforms as needed.



Orange Alarm: When receiving an orange alert parties are expected to make proportionate enquiries within their jurisdiction and feedback any relevant findings to the originator.

There is an expectation that any National Platform acting on an Orange Notice will document their relevant findings.

Below the Action Card text is shown:

Niveau:	Description:	Procedure:
Orange	<p>Concrete indications from:</p> <ul style="list-style-type: none"> Persistent unexplained irregularities in betting patterns / odds movements <p>Reliable information via:</p> <ul style="list-style-type: none"> Media Social Media Stakeholders Whistleblower 	<ul style="list-style-type: none"> Collection and documentation of information Immediate contact to specific stakeholders e.g. Police, Sports federation etc. Notification to international stakeholders including Groupe of Copenhagen members. Documentation of conclusion - return to normal level with Green Notice.

Red:

Red: (Highest alert): This level is only used when match fixing is imminent or has just occurred. If there is concrete knowledge about match fixing, it is important that alerts are shared quickly, efficiently and to the right recipients. In this way, it is ensured that the recipient will have the best opportunity to take appropriate actions concerning their field expertise.

Red Alert: Sending a red alert must be made according to guidelines for secure communication. It is important to point out that information shared with a wrong recipient or compromised due to insecure communication could have a significant detrimental impact on any investigations being carried out by Law Enforcement or other key stakeholders.

Red alarm: When receiving a red alert, it is essential that stakeholders focus on collecting and documenting any findings as these must be considered evidence. If a police investigation is likely to occur, they will need the gathered material. Information collection and any further actions taken in relation to the incident should therefore be carried out in close cooperation with the appropriate authority.

Below the Action Card text is shown:

Level:	Description:	Procedure:
Red	<p>Evident proof of match fixing</p> <p>Information via:</p> <ul style="list-style-type: none"> Media Social Media Stakeholders Whistleblower 	<ul style="list-style-type: none"> Collection and documentation of information for evidence. Contact to the relevant authority. Notification to international stakeholders. Documentation of conclusion - return to normal level with Green Notice.

3. Monitoring Level (Risk Assessment):

In order to identify and prevent match fixing, it is the recommendation of the working group to use analytical and targeted risk assessment. In order to utilize stakeholder resources in the best possible way, it is recommended that, based on a proper risk assessment, current sports events are divided into categories that provide a differentiated level of monitoring. Such a risk assessment can be recommended, for example, in planning the monitoring of major sports events or simply by designating the particularly vulnerable sports.

Depending on the type of organization you represent, there will be different circumstances that relate to this form of risk assessment. However, the following overall characteristics can be emphasized by assessing the risk associated with betting on sports¹:

Sports factors:

- The tournament contains a playoff (opportunity for "non-purpose" matches)
- Lower league
- Low wages (or finances based on sponsorship only)
- Low media attention
- Sport is "unknown" in large parts of the population
- Past cases related to a team, a competitor, owner, convicted or suspected of match fixing.

Societal factors (countries / regions):

- General living standard
- Low / High Corruption Index in the country concerned (<http://www.transparency.org/cpi2015>)

Betting-related factors:

- Who is the betting provider?
- Where is the betting provider resident?
- What kind of bets are offered (live betting, Asian handicap, online, kiosk based, etc.)

The above-mentioned factors must be combined with specific knowledge about:

- Number and types of bets, the individual sports (inside information), the number of bookmakers offering bets etc.

The table below shows an example of risk assessment in relation to a number of Danish sports²:

Sport	Risk assessment	Profit	Number of betting providers
Football	High	High	360
Ice hockey	High	Medium	300
Handball	High	Medium	<i>Awaits answer</i>
Basketball	High	Medium	<i>Awaits answer</i>
Volleyball	High	Low	<i>Awaits answer</i>
Floorball	High	Low	80

Based on a thorough assessment, three levels of surveillance can be established:

Normal Surveillance:

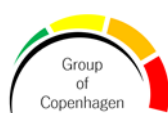
- Normal daily operation for platform members.

Strengthened surveillance:

- Members of the National Platform are notified.
- Intensify the surveillance via OSINT (Open Source Intelligence)
- Lowering the threshold for the automatic alerts.
- Communicate with relevant international partners.
- Identify Single point of contact (SPOC) amongst various stakeholders (e.g. IOC, federations and/or Ministry for Sports).

¹ The list below is not in any way exhaustive – it is simply meant as inspiration when pointing out key characteristics

² Statistics collected in cooperation with relevant stakeholders during 2017.



- Consider the possibility of contact to relevant:
 - Sports teams
 - Officials
- Encourage organizers of sporting event to start systematic collection and documentation of relevant information.
- Inform the National Police.

Maximum surveillance:

- Increased betting market monitoring and development of odds, etc.
- Close dialogue with platform stakeholders, both nationally and internationally. Frequent distribution of alerts and notifications.
- Increased communication relevant non-platform stakeholder.
- Systematic collection and documentation of relevant information.
- Identify Single point of contact (SPOC) amongst various stakeholders (e.g. IOC, federations and/or Ministry for Sports).
- Encourage organizers of sporting event to start systematic collection and documentation of relevant information.
- National Police is informed.
- Europol / Interpol is informed.

The surveillance levels and suggested actions mentioned above can be found in the hand book tool: Action Card: Surveillance Levels.

4. Secure encrypted communication:

In order to limit the correspondence between the various stakeholders, ADD's recommendation is to introduce a "no-answer policy" - in other words, stakeholders should only respond to an alert / inquiry if they have a contribution. Thus, "courtesy mail" without operational content should not be sent.



For such a no-answer policy to be maintained, the stakeholders should use a communication tool that is able to inform the sender who has received the attached material, downloaded it and, if necessary, the answer to the inquiry.

ADD currently uses the 256-bit encrypted system "Citrix ShareFile". In addition to security and overview, this system provides the user with the ability to control a wide range of internal communication parameters. For instance, the system can create a number of dedicated folders for sharing information. In the long term, it will probably be advisable to create more subfolders for sharing other forms of communication, including guides, statistics, etc.



5. The Alert template:

When information is shared between the different stakeholders, alignment and recognition are important elements. Therefore, ADD has prepared the following template for sending messages between the various stakeholders:

Orange Notice

Alert Matchfixing					
Information from:	Type here.			Date:	Select date.
Evaluation					
Evaluation of source:	A <input type="checkbox"/> Reliable	B <input type="checkbox"/> Often reliable	C <input type="checkbox"/> Often not reliable	X <input type="checkbox"/> Untrusted source - Cannot be validated	
Evaluation of Information:	1 <input type="checkbox"/> Truth – no doubt	2 <input type="checkbox"/> Information known by source	3 <input type="checkbox"/> False or malicious information	4 <input type="checkbox"/> Cannot be confirmed	
Information regarding					
Matchfixing:	<input type="checkbox"/>	Betting:	<input type="checkbox"/>	Other:	<input type="checkbox"/> <i>If 'Other' please add description: Type here.</i>
					Log-book category: Chose category.
Sport:	Type here.		Level:	Type here.	
Club/player:	Type here.				Date/time of event: 03-11-2017
					Country of event: List or type.
Detailed information					
Type here.					
National Platform					
Notification:	Type here.				
Handling code:	O <input type="checkbox"/> Open <i>Lawful sharing permitted.</i>		R <input type="checkbox"/> Restricted and Confidential <i>Sharing only with permission from originator and with conditions (see below)</i>		
Conditions for sharing:	Conditions for sharing.				
Shared with:	Type here.				
Notes:	Type here.		Contact for further information:	Type here.	

NOTE: This Notice is intended only for the named recipient(s) above and will contain information that is privileged, confidential and/or exempt from disclosure under applicable law. If you have received this Notice by error, or are not the named recipient(s), please immediately notify the sender and delete this message.

The design of the template emphasizes the balance between a clear expression, but also a design that allows for detailed information.

Fields have been added relative to source and informant evaluation. Such an evaluation will help to strengthen the seriousness of the content of the information provided, as well as force the sender to relate to the source and information. The template also includes fields for direct contact information,

requests to recipients, listing of planned actions as well as information about whom information is shared with³.

The template is also provided with predefined fields in order to control the workflow during completion.

For example, color selection has been added by double-click, automatic date field, tab shift between the active fields, etc. The idea is that the form is filled in and then converted to PDF and finally shared with relevant recipients in a secure encrypted manner using the Citrix ShareFile system.

Evaluation field (Template):

In order to strengthen the product for intelligence purposes, a section dealing with the evaluation of source and information has been introduced. The validation tells the recipient of the immediate assessment behind the choice of alert / alarm level.

Globally, there are a number of different validation systems, but in a Danish context it makes sense to use the 4x4 system, the same as used by Danish Police (and Europol). Below is the validation key listed:

Source:

A: Credible - or historically reliable.

- No doubt about the credibility of the source Official government stakeholders e.g. Police, Gambling Commission or Tax Authorities is to be considered category A under normal circumstances. (Bias-free)

B: Mostly reliable.

- A source that in most cases have been reliable. (Possibility that the source will pass information under influence of bias)

C: Mostly unreliable.

- Informant/source often speaking untrue e.g. several times shown not to be trustworthy.

X: Cannot be considered.

- If the source cannot be placed in any of the above-mentioned categories choose X e.g. when working with new unknown source.

Information:

1: True - without doubt.

- When there is no doubt what so ever about the accuracy of the information received from source. Information from government database is considered to be level 1 information.

2: The information is known from the source

- When information is known by source e.g. first-hand knowledge, participance or eye witnessed.

3: False or malicious information.

- When it is established that the information is false. Can for instance be used as evidence in order to show criminal intent etc.

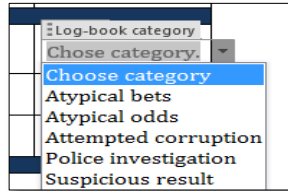
³ The template is designed in MS WORD and is using macros. Therefor the user must enable macros in order to use drop boxes etc. The template will be uploaded to the Citrix Sharefile from where it can be downloaded and used.

4: Cannot be confirmed.

- When the information is not known as first-hand by the source/informant or the information cannot be backed by previous intel.

Log-book category (Template)

On the template under the headline *Information Regarding* there is inserted a drop-down menu. Here the sender has the possibility to choose the adequate category analog to the definitions found in the analytical tool *The GoC Log-book*.



Handling Codes (Template)

The possibility to control the flow of information is an important issue. First of all it will ensure that restricted, confidential or personal data will not be shared with non-relevant stakeholders. Furthermore can the use of handling codes be seen as a tool that will strengthen the mutual trust between the various National Platforms and other stakeholders if used.

Handling Codes can be described as an essential methodology that will help to ensure the above mentioned key factors when communicating. It is of the utmost importance that the sender can trust that shared information will be handled according to their instructions and intentions. Basically, when using handling codes, it is the privilege of the sender to choose how, with whom and under what circumstances the information is shared.

In order to keep a simple and yet effective system we have decided to work with two types of handling codes as seen below:

Handling code:	<input type="checkbox"/> Open <i>Lawful sharing permitted.</i>	<input type="checkbox"/> Restricted and Confidential <i>Sharing only with permission from originator and with conditions (see below)</i>
Conditions for sharing:	Conditions for sharing.	

When choosing handling code: O (Open) the sender hereby gives the recipient the possibility the share the information freely with whom they choose. When sharing information always evaluate the nature of the content and take legislation regarding personal data protection in to consideration before passing on information.

If choosing the handling code: R (Restricted and Confidential) the information is send strictly to the recipient stated on the template. It is the privilege of the sender to add certain conditions for sharing for example:

1. For national platforms only – can be shared with National Police
2. Can be shared if permission given by sender, contact xx@aa.dk

Be aware that there are no technical mechanisms in place that can hinder a Notice-recipient from sharing a template categorized with the handling code **R**. The admin⁴ of the Citrix Sharefile system will though be able to track the single template shared, uploaded or downloaded.

⁴Admin of the Citrix Sharefile folder: Anti Doping Danmark, Intelligence Manager.

