Northwest Atlantic  Fisheries Organization

Serial No. N6387

NAFO/FC Doc. 14/22
(Adopted)

36th ANNUAL MEETING – SEPTEMBER 2014

NAFO Information Security and Management System (ISMS)

At the STACTIC Intersessional meeting in May 2014 the Secretariat was requested to look into the NEAFC application of an Information Security and Management System (ISMS) as it was technically evaluated by the Joint Advisory Committee on Data Management (JAGDM) and report back to STACTIC on its potential application to NAFO.

At the JAGDM meeting in June 2014 the Secretariat took this up with the participants under agenda item 6.a and it was agreed that the Interim Chair would write a letter, with input from the participants, for the NAFO Secretariat to present to STACTIC in September on why NAFO may need an ISMS. This letter is attached. In her letter, the Interim Chair advises that NAFO proceed with developing an ISMS.

If STACTIC decides that NAFO should follow this advice, it is important to determine guidelines for the work. The ISMS of NEAFC is in line with the ISO 27001:2005, the current version of this standard is ISO 27001:2013. It is important to know if NAFO will start the work in line with the ISO 27001:2013, follow another standard or not follow any standard. The Interim Chair conveyed to the Secretariat the availability of JAGDM to assist in this preliminary determination. If needed a specialised meeting within JAGDM could take place in 2015 to exclusively address developing a possible NAFO ISMS.

If STACTIC decides that NAFO should consider an ISMS, it would also be useful to get a picture of how NAFO's current information technology (IT) system compares with best practices. The Secretariat suggests that this could be addressed by an external audit of NAFO's current IT-system.

The Secretariat thereby suggests that:

1. STACTIC approve in principle that NAFO consider the implementation of an ISMS.
2. STACTIC request the assistance of JAGDM to determine guidelines for any ISMS;
3. The Secretariat consider an external audit of NAFO's current IT-system; and
4. The issue of a NAFO ISMS be an item on the next STACTIC agenda.

To the NAFO Secretariat Bergen 22 August 2014

From JAGDM

At its June 2014 meeting, JAGDM was asked to give advice to the NAFO Secretariat concerning why NAFO needs an Information Security Management System (ISMS).

When the IT-system of NAFO first was developed many years ago, security and confidentiality aspects were addressed by an annex in the CEM. This covered the needs at that time. However, the handling of IT-information in NAFO is no longer limited to sending data between Contracting Parties and the NAFO Secretariat using secure lines and storing data in the computer at the office of the Secretariat.

Moreover, the NAFO website raises further concerns. People with several needs and wishes may want to access and have information presented on the website, and in some cases may also want to input data into the system.

Without an overview and some formalization of the total information handling within NAFO, it is not possible for the Contracting Parties to know what the security and confidentiality policy of the organization is. Currently the NAFO Secretariat has followed its own policies without any guidelines, other than the Annex II.B of the CEM. Although the NAFO Secretariat tries to follow industry standards, it is not clear whether these standards would be acceptable to all Contracting Parties, particularly those that might have different standards in their own countries. This raises risks that certain confidential data may be accessed incorrectly and the organization get negative reactions.

NAFO does not need to have an ISMS in line with a standard such as NEAFC has done. However if NAFO is going to have an overview and formalize its information security it is beneficial if it is done in line with a standard, specially taking into consideration that NAFO has many Contracting parties that might have very different systems in their own countries.

Data stored on the NAFO IT-system largely contains copies of data also stored by the Contracting Parties so new copies of data could be submitted if ever needed. However the Port State data is different. The only copy of this data is only stored on the Secretariat's servers.

In a modern IT-world it is very important to be sure that one has a system that is secure enough to give the organization the decided level of business continuity.

Data has to be classified correctly and from that handled according to the risks identified.

Having an ISMS will not necessarily give the organization a higher or lower level of security, but it makes it possible for the Contracting Parties to know what the status is and from that decide if changes are needed. There will be guidelines for many situations that are meant to help the employees to take the correct decisions.

Preparing the ISMS for NEAFC has been a lot of work and if NAFO is planning an ISMS there has to be people in the Secretariat doing the information-finding job. It is important that one starts with an assessment of the current situation.

If NAFO wishes to use an international standard we recommend that NAFO follow the same ISO standard as NEAFC uses. This will help harmonization between the two organizations. If so NAFO should most likely use the latest ISO 27001:2013 standard that NEAFC will be updating their ISMS to presently.

Best regards

For JAGDM - Ellen E. Fasmer, Interim chair