TIBER-NO

Threat Intelligence Based
Ethical Red-teaming
Norway

NORGES BANK

TLP: Amber

Project.: 22-131
Document no.: 22-5067

November 2022

WHITE TEAM AND TCT RULES OF ENGAGEMENT

Version 1.2

This document supplements the test process overview and describes rules of engagement and practical issues related to the TIBER-NO test process and details in the cooperation between the entity/White Team and the TCT. The document is targeted at the specific entities performing the TIBER-NO test process. The document is distributed to TCT and WT members after completion.

Contents

1 Code name

Code names are used in sensitive documents instead of the TIBER-NO participant's real entity name. In case of a leak or a security breach, the use of code names makes it harder to link the sensitive information to the tested entity.

For the code name to be effective, there must be a strict discipline following the guidelines below:

- Use a code name that is not logically linked to or derived from the entity's name so the code name should not be meaningful.
- Always use the code name in sensitive documents but do not use the code name in documents or in communication that contains information that can be linked back to the organisation.
- Never use the code name in conjunction with the organisation's real name such as in emails and meeting invitations where you have sender/recipient/copy using "xx@entityname.no."
- In case the code name has been disclosed or used in conjunction with the organisation name, the TCT can require a new code name, depending on severity. In such cases, the TCT will ensure the new code name is changed accordingly in existing documents.

The code name [CODE NAME] has been chosen.

2 Main principles for good cooperation

All parties involved in the TIBER-NO test shall take a collaborative, transparent and flexible approach to the work. Focus shall be on maximizing the tested entity's learning from the red team testing experience. A prerequisite for a successful test is close cooperation between the WT and the TCT during all phases of the test. Information sharing is key to ensure tests run smoothly. Any issues, resource constraints, or similar must be addressed in a timely fashion. In general terms we commit to:

- Follow the principles of TIBER-NO as described in the TIBER-NO Implementation Guide.
- Respect and strive for proper planning.
- Be honest and transparent.
- Collaborate to succeed.
- Always inform in a timely fashion of deviations to original planning, see also section "Changes".

3 Organisation

The overall role of TCT is to manage, operationalise and monitor the TIBER-NO programme and each of the tests carried out in the programme to ensure uniform, high-quality tests as described in

the "TIBER-NO Implementation Guide". For this purpose, the TCT team is constituted of several people, including a dedicated TIBER Test Manager (TTM) for each test (see "Contact" section).

Meetings between TCT and [CODE NAME] will always be organized via the TTM and WT lead. In general, the TTM will function as the point of contact for all identified issues, escalations etc. that needs to be discussed outside regular status meetings, see section "Meetings".

4 Confidentiality

The information produced and discussed during the TIBER-NO test must be protected and kept confidential. The TCT adheres to the Norwegian Information Protection Instructions ("Beskyttelseinstruksen") and will classify documents accordingly. Sensitive information assets produced by other entities and sent to the TCT will be treated as "in confidence" (FORTROLIG) or "strictly in confidence" (STRENGT FORTROLIG).

To further minimize the risk of exposure, the TCT will follow the below principles:

- Traffic Light Protocol (TLP) will be used according to FIRST Standards Definitions and Usage Guidance - Version 2.0, https://www.first.org/tlp/.
- Highly sensitive data (such as test results or findings) are stored only by [CODE NAME] to avoid unnecessary concentration risk. Such data, including Red Team test reports, should be reviewed by the TCT on a physical format only.
- All members of the TCT have been cleared for employment as regulated by Sentralbankloven § 2-15
- The TCT is responsible to ensure their physical working environment (such as Norges Bank's offices or home offices) are suitably secure with limited access.
- TCT keeps a "clean desk"-policy.
- TCT laptops are fully encrypted and hardened following Norges Bank internal security policies
- Confidential printed documents are stored in locked cabinets.
- Confidential digital documents stored either in Norges Bank archival system or on MS Teams are protected with relevant access restrictions applied, according to Norges Bank internal security policies.
- Documents produced by the test participants are stored in MS Teams and moved from MS Teams to Norges Bank archival system after the TIBER-test is concluded.
- All meeting invites, unless otherwise agreed, are made "private".

The TCT (including its steering committee) will not share any information about a specific TIBER-NO test with other authorities (including other central banks) without having consent from the testing entity. The tested entity is the legal owner of all material produced during the test and responsible for sharing this material with its competent authorities (for instance Finanstilsynet), if required.

Likewise, [CODE NAME] has decided on the following principles to minimize risk of exposure:

- [text input [CODE NAME]
- [text input [CODE NAME]

5 Communication platforms

For sharing of documents between WT and TCT the primary channel is MS Teams. The main purpose of using MS Teams is to ensure appropriate access control, logging etc. Emails should only be used to share information not considered sensitive. In general, sharing of documents in emails should be avoided, as this will increase the risk of inadvertently sharing sensitive information e.g. code name specifically to "outsiders".

To ensure traceability and documentation and to avoid misinterpretation, phone calls should only be used as means of "light" information sharing and planning. Usage of any additional communication tools must be mutually agreed, and such tools should be treated as a phone call.

Meeting invitations made by TCT shall only contain general descriptions in the subject field to avoid unintended disclosure, such as "Meeting according to plan". Invitations will be made “private” to protect any details about the meeting in the invitation itself.

6 Status meetings

Status meetings will be held approximately every fortnight in the preparation phase and may be supplemented with additional meetings. In the Targeted TI phase, the Red Team test phase and the Closure phase, the status meetings will be arranged as needed and as a supplement to TI and RT meetings and other meetings arranged by the WT lead. The meeting frequency in all phases can be changed if all parties agree.

Status meetings will normally be held virtually or, if agreed, physically at Norges Bank’s facilities. Meetings will take place on [day of the week to be discussed] unless otherwise decided. Each organisation decides who will attend on behalf of their organisation.

The generic agenda for the status meetings is:

1. Overall status from [CODE NAME]
2. Overall status from TCT
3. Detailed status on ongoing activities in the plan, including coordination
4. Start of new activities in the plan, including coordination
5. Follow up on progress
6. Other issues

TCT will write decision minutes from the status meetings and maintain a log with ongoing tasks. TCT will strive to publish the updates shortly after each status meeting on MS Teams and inform about new/updated material by email.

7 Changes

If there are deviations, for instance from the original planning, this should be discussed with the TCT. It is critical all relevant stakeholders keep each other informed at all stages to ensure the test runs smoothly and any issues, resource constraints or similar are addressed in a timely fashion.

In general, changes will be discussed, coordinated, and agreed upon on status meetings and documented in the minutes. Any deviations or changes decided outside status meetings must be fully documented.

8 Escalation

Escalations related to time and quality of the test may be needed, for instance during the active red team phase, to ensure progress and a satisfactory outcome of the test.

Escalations shall go through the WTL and the TTM at TCT.

9 Ethical rules for applying test findings

TIBER testing is one of the most advanced and comprehensive security testing methods available. It is likely testing will uncover vulnerabilities and weaknesses in the entity. Some of these vulnerabilities may be directly or indirectly caused by human error, such as falling for social engineering attacks like phishing. A premise for TIBER-NO testing is that any such uncovered errors shall not be used as basis for disciplinary action. If any such actions are made known to the TCT the test can be invalidated.

10 Contacts

Contacts for both organisations are listed in a separate document and must be kept updated. Any changes to the contact list must immediately be reported to TCT who will decide if the changes require action, for example removing access to MS Teams.

Document change log

Version	Date	Comments
1.0	xx.xx.2022	Initial version

Template change log

This section can be deleted when the template is used.

Version	Date	Comments
1.2	15.12.2022	Moved White Team table to separate document and added Document change log
1.1	30.11.2022	Updated and adapted for TIBER-NO usage
1.0	28.11.2022	Initial version from TCT-DK