NORGES BANK

TIBER-NO
Risk Management Guidance

Version 2.0

TLP:CLEAR

About this document

A TIBER-NO test constitutes elements of risk for all parties, owing to the criticality of the target systems and the people and processes involved a test. The possibility of causing negative incidents, such as a denial-of-service incident, an unexpected system halt, damage to critical live production systems, or loss, modification, or disclosure of data, demonstrates the need for active and robust risk management.

This guide can assist an entity to perform a test with an active and robust risk management and to document appropriate controls, processes, and procedures. It helps a test to be performed in a controlled manner. Possible risks need to be identified, analysed, and mitigated or accepted according to best practice. This guide is based on learnings from prior TIBER-tests and other inputs. It does not represent an exhaustive list of all relevant areas for risk management. Other TIBER-NO guides include ideas for how to reduce risk and should also be consulted for this purpose.

Many of the ideas for risk reducing activities can in some cases reduce the quality or learning outcomes of the test and should therefore only be employed if needed to reduce risk to an acceptable level.

It is assumed the entity uses its own risk management framework for documenting and addressing the risks identified for its own TIBER-NO test.

Disclaimer

The TIBER-NO Cyber Team of Norges Bank (TCT) can under no circumstances be held accountable for the risk management of a TIBER-NO entity. The full responsibility to conduct proper and timely risk management in line with best practices rests solely on the entity undergoing the test. This document is only a guide to aid in the risk management planning.

1. Legal and Providers

Due to the nature of a TIBER test, the TI and RT Providers may gain significant knowledge about exploitable vulnerabilities and potential security breaches in infrastructure and systems for the tested entity.

Risk ideas:

- Liability if the provider makes a mistake, such as disrupting production systems or information leakage.
- Premature disclosure of the test due to lack of experience or skills within the RT team
- Incident escalation beyond the scope of the test
- Changes in personnel of RT testers during the test, especially for the RT lead.
- Red teaming exercises may need to comply with various regulatory requirements, such as data protection laws or industry standards. Failure to adhere to these requirements could result in regulatory fines or penalties.
- Privacy Violations: Red teaming often involves accessing sensitive information or systems, which could potentially infringe upon individuals' privacy rights if not handled appropriately.

Ideas for risk reducing activities:

- Provider includes insurance against mistakes or negligence.
- Usage of non-disclosure agreements (NDA)
- Require compliance with regulatory requirements within all areas of the business.
- Safeguards to restrict access to confidential material the provider gets access to. Examples can be financial statements, insider information, or legal issues.
- Enforcing a data retention policy towards the providers
- Data Protection: Handle sensitive information and data obtained during red teaming exercises with the utmost care and in compliance with applicable privacy laws and regulations.
- Inform employee union representatives of possible testing.

2. Ethics and reputation

Ethical rules set the barriers for which methods the TI provider might use to gather intelligence and which methods the RT provider might employ to conduct its attacks. An actual threat actor will attempt to use methods not ethically possible in a TIBER test. Boundaries need to be clearly defined for what might be acceptable practices in the test. A lack of protection of privacy and personal data or revealing information based on intelligence gathered by the TI provider might lead to loss of reputation or customer confidence.

Risk ideas:

- Employee distress leading to negative psychological impact caused by the test, such as an employee falling for social engineering attacks, such as phishing, vishing, or impersonation. This should include both human error or what might be perceived as human errors.
- Providers may want to share experiences from the test, make references or use the test for marketing. It is up to the tested entity to decide what is permissible to

share, but this information should only be shared once the test is completely finalized.

- If TIBER-testing is perceived as intrusive or unethical by stakeholders or the public, it could damage the organization's reputation or erode trust.
- Any mishandling or misuse of red teaming exercises could attract negative attention from media outlets, leading to reputational damage and customer confidence.
- If the details or outcomes of red teaming exercises are disclosed to external parties without proper authorization or consent, it could lead to reputational damage for the organization. This includes the risk of negative media coverage, loss of customer trust, and damage to business relationships.

Ideas for risk reducing activities:

- Ensure managers of targeted employees for phishing/vishing campaigns are aware of these activities.
- Remove employees from list of targets who might be adversely affected.
- Swift and close follow-up of employees who have fallen for targeted campaigns.
- Define general criteria or process for WT review contents of phishing e-mails to ensure they are acceptably crafted, such as not using personal information, adequate type of language or other specific content to avoid.
- The providers must follow all international and national legislation and regulations.
- Follow the highest standard for ethical conduct (OSIRA, CREST Code-of-ethics or similar)
- Information or privileges gained can only be used in this specific engagement.
- Informed Consent: Ensure all participants, including employees and stakeholders, are aware of and consent to the red teaming exercises beforehand, including the potential risks involved.
- Transparency: Clearly communicate the purpose, scope, and rules of engagement for red teaming exercises to all relevant parties to mitigate any misunderstandings or misconceptions.
- Professional Conduct: Conduct red teaming exercises with professionalism, integrity, and respect for all parties involved, avoiding any actions or behaviors that could be considered unethical or inappropriate.

3. Crisis and incident escalation

It is expected that a TIBER test will trigger incident escalations within the tested organisation. This section covers the risks and related procedures put in place to ensure the White Team is in control of any escalations related to testing.

Risk ideas:

- Escalations are done outside of documented routines, such as directly to police without involvement of a CISO.

- WT not available when the incident escalates, such as during night-time, weekends or holidays.

Ideas for risk reducing activities:

- Ensure WT has sufficient knowledge of practical handling of business procedures for handling security incidents, both general and system specific procedures. This can be achieved by including a subject matter expert (SME) in the extended white team.
- Develop use cases to understand how the WT can manage incidents. The use cases should provide answers to when tests should be continued, and which type of incidents should stop the test. Identify where in the "information chain" escalations should be stopped and how to respond to avoid disclosure of the test. The WT must be able to stop escalations to law enforcement and other authorities. In general, it is better to reveal only a partial truth, for instance this is just a normal phishing test, or a specific test related to server vulnerabilities instead of announcing it is a TIBER test.
- Procedures for managing incidents and control critical incidents which may arise because of testing. A natural outcome of the test activity is for BT to detect some of the attack activity and escalate incidents. The WT needs to be included in the process and liaise with management or similar functions to:
    - Define procedures to clarify if incidents are related to the test
    - Understand trigger actions and ensure escalations internally can be "intercepted" and controlled.
    - Set aside time for this kind of activity, also due to false positives incidents
    - Be available for handling escalations whenever needed (24/7)

4. Operational red teaming

At all times during a test the WT must be in control of red-team activities. The WT needs to have a clear set of communication guidelines and to establish a mutual understanding of the entity's risk appetite as well as boundaries for red team activities. Lack of proper risk management might lead to unexpected or unknown activities and events. Potential incidents such as system unavailability, deletion of data, or inadequate log documentation should be addressed.

Key systems and services identified in the scope together with supporting IT-systems should be identified and included in the risk assessment.

Risk ideas:

- Testing activities interfere with critical activities, such as pay-day, freeze periods, deployment of system upgrades, other testing activities not aware of the TIBER test, IT Christmas party, etc.
- Revealing information between parties involved in the TIBER test.
- Challenges getting in contact with needed parties on short notice.
- RT gets access to highly confidential material, for instance financial statements/insider information/legal issues.

- Leg-ups are delayed or compromised.

Ideas for risk reducing activities:

- Have members of the White team with extra attention available or avoid known periods which pose too high a risk to conduct test in live production systems.
- Analyse what could make systems unstable based on prior experience. For instance, large amounts of data passing through an application or other knowledge gained from past incidents.
- Secure ways of communication between WT and TI/RT to ensure sufficient confidentiality level. Consider which type of communication is allowed depending on purpose, such as physical meetings, phone, Teams, Signal, secure mail etc.
- Define how hosting of attack infrastructure like Command & Control servers shall be set up, including access to infrastructure from test participants.
- Define procedures for protection of information at rest or in transit. Examples can be artifacts, logs, test results, evidence, and screenshots.
- Document RT's internal procedures for complying with the Rules of Engagement with the entity being tested.
- Regular updates of detailed contact information for all participants, such as contacts in TCT, TI, RT and WT. Include information like roles, deputies, and mobile phone numbers. Note also possible times contacts are unavailable, such as planned holidays, on/off business hours, which RT testers are active and when.
- Frequent regular status meetings during the red team test execution, such as daily and weekly meetings.
- Define what type of information to expect from RT on a regular basis. This can be overview of progress for each scenario such as using visual flow charts, changes to RT test plan, risk considerations for upcoming activities, the frequency of delivering log updates or other material indicating ongoing success level.
- Document escalation procedures, such as between RT lead and WT Lead, and between RT lead and RT team.
- Approval hierarchy with primary contact and deputy, for instance if WT Lead suddenly becomes ill or unavailable. If no response can be obtained, how should RT continue?
- “Red button” to stop the test immediately and who can approve.
- Operational limitations, such as only allow to communicate with RT Command & Control systems and only over secure line, or web shells to be password protected.
- Conduct thorough due diligence of in-scope systems prior to any testing to ensure that backup and restoration capabilities are in place.
- Document disruptive activities may not be performed, such as locking out users (if for instance a password spraying attack has the potential to lock out users), deleting/moving files or changing security posture/setup/policies.
- Implement a “kill switch” for software implants or backdoors.

5. Operational blue teaming

A key success factor for a TIBER test is to avoid disclosing the test to the Blue Team. If a test is disclosed, the Blue Team will most likely adjust its behaviour, such as shifting to a state of alert, leading to misguiding test results.

Consideration must be given to the workload of the Blue Team who risks being overloaded with activities to defend itself against test attacks, increasing the risk an actual attack is not properly handled. The WT might address the risk of disclosing the test to the Blue Team, for example, by utilising cover-up stories or agreed-upon procedures for stopping and pausing a test.

Risk ideas:

- Not sufficient resources or overwhelmed by stress to handle actual attacks, since BT is overloaded with TIBER test activities.
- BT uses an extended number of hours or overtime and work during weekends
- Blue team members may misinterpret the findings or lessons learned from red teaming exercises, leading to ineffective or misguided security improvements and strategies.
- Devoting time, personnel, and resources to participate in red teaming exercises can divert attention away from other critical security tasks and projects, potentially leaving gaps in day-to-day security operations.

Ideas for risk reducing activities:

- Define actions if a real attack happens simultaneously.
- Make a strategy for handling BT inquiries, such as prepare cover stories within the WT.
- Prepare leg-ups well in advance to not be noticed by the BT, such as to prepare laptops and user accounts no longer in use due to a consultant who has finished an assignment. The laptop will have “normal” traffic and history, like shares visited and security identifiers (SID’s) registered on the laptop and mirrors a normal attack situation.

6. Clean up

Clean-up activities must be performed after the test has been completed, for example to remove malware, backdoors and other infrastructure used for the test.

The WT, any service provider and RT Provider must ensure all user accounts and credentials, infrastructure and software, and test prerequisites are thoroughly documented for the benefit of clean-up. Each item should be reviewed and examined after test completion. These items are therefore implicitly risks that should be managed.

Risk ideas:

- User accounts and credentials used during the test are not discontinued.
- Software or infrastructure is not removed.
- Lack of performing clean-up activities on RT side.

- Firewall or infrastructure changes are not revoked.
- Vulnerable software is not patched swiftly enough.
- Data retention at provider is not defined or enforced.

Ideas for risk reducing activities:

- Document all required clean-up activities, both before and during the test.
- Perform and document clean-up activities such as removal of malware, trigger kill switch/self-destruct mechanisms, ensure reboot for file-less malware, remove phishing e-mails, close or reset accounts and credentials
- Remind all test persons involved in the test to delete documents no longer needed, such as data extracted during the test, Red Team test report, and other sensitive information.
- Discuss appropriate procedures for managing any future restore from backups containing malware or tools installed during test.

7. Project management

A TIBER-test should be run as a project by the WT. Traditional project risks are relevant, including risks of failing to deliver on time, cost, and quality.

Risk ideas:

- Delay of activities
- Disclosure of test results (deliberately or inadvertently)
- Financial risk (overspending, unexpected activities or delays)
- Change of resources due to sickness, leave, leaving the company etc.
- Lack of contingency plan if the test is detected.
- Quality objectives for the test are not reached, due to various reasons including resource management and people management.

Ideas for risk reducing activities:

- Weekly meetings with WT and TCT
- Follow-up on project plan regularly
- Identify potential deputies.
- Integrate risk management into the daily operational project management routines.

8. Other

Any relevant risks outside scope for the sections above should be addressed here.

Change log

Version	Date	Change
2.0	23.05.2024	AH: Extensive rewrite with examples included from previous Supporting Document
1.0	27.11.2023	Initial version