

Addendum TIBER Service Procurement Guidelines for ART

This addendum is intended for financial institutions seeking to hire a threat intelligence provider or red team provider for an ART-NL test. For this procurement procedure, the [TIBER-EU Service Procurement Guidelines \(TSPG\)](#) must be used until further notice, with this addendum as a binding supplement.

TI provider requirements for ART (module 4) (replacing table 1 in the TSPG, page 11)

Who	Requirements
TI provider (at company level)	<ul style="list-style-type: none"> • For the staff assigned to the test: demonstrably relevant portfolio of comparable previous assignments related to red-team testing. • Having access to (private or commercially available) threat intelligence databases, at minimum containing up to date threat actor profiles and their TTPs. • Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence, etc. • Capacity to form a TI team of at least two persons, with additional capacity available if needed. • No previous or current services delivered for the entity, that would present a conflict of interest for the Service Provider when conducting an ART test.
Threat Intelligence Manager – responsible for the end-to-end management of the threat intelligence for a TIBER-EU test	<ul style="list-style-type: none"> • Lead and oversight of the TI provider’s activities for delivering an ART test are ensured by a Threat Intelligence Manager. • The Threat Intelligence Manager is able to explain advanced, technical TI subjects to technical experts (i.e. members of the Blue Team) and to non-experts in an understandable manner, delivering actionable threat intelligence for the institution. • Sufficient experience of the Threat Intelligence Manager in threat intelligence. At least three years of experience in threat intelligence. • Intermediate understanding of the workings of the financial sector, its processes, underlying systems, sectoral challenges and threat landscape. • Up-to-date CV to be provided to the entity, specifically in delivering threat intelligence for red team testing activities. • Background checks on the Threat Intelligence Manager are conducted by the TI provider (as a minimum), including those required by the national authorities. • The Threat Intelligence Manager should have appropriate recognised qualifications and certifications for threat intelligence, as defined in the TIBER-EU indicative qualifications list.
Threat Intelligence Team (all members of the team, except	<ul style="list-style-type: none"> • Sufficient experience of the Threat Intelligence Team members. Expectation for each member: at least two years of experience in threat intelligence. • Basic understanding of the workings of the financial sector, its processes, underlying systems, sectoral challenges and threat landscape.

for the Threat Intelligence Manager) – responsible for delivering the threat intelligence for a TIBER-EU test

- Up-to-date CV for each member of the team to be provided to the entity.
- Multi-disciplinary composition of the Threat Intelligence Team, with a broad range of skills including OSINT, HUMINT and geopolitical knowledge.
- Background checks on each member of the Threat Intelligence Team are conducted by the TI provider (as a minimum). Enhanced background checks are conducted as required by the national authorities.
- The Threat Intelligence Team members are able to explain advanced, technical TI subjects to technical experts (i.e. members of the Blue Team) and to non-experts in an understandable manner, delivering actionable threat intelligence for the institution.
- Ideally, the Threat Intelligence Team should have experience in delivering threat intelligence for red team tests.

RT provider requirements for ART – for threat intelligence (ART module 3)

Who	Requirements
RT provider (at company level)	<ul style="list-style-type: none"> • For the staff assigned to the test: demonstrably relevant portfolio of comparable previous assignments related to red-team testing. • Having access to (private or commercially available) threat intelligence databases, at minimum containing up to date threat actor profiles and their TTPs. • Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence, etc. • No previous or current services delivered for the entity, that would present a conflict of interest for the Service Provider when conducting an ART test.
Threat Intelligence Manager – responsible for the end-to-end management of the threat intelligence for a TIBER-EU test	<ul style="list-style-type: none"> • Lead and oversight of the RT provider’s activities for delivering an ART test are ensured by a Threat Intelligence Manager. • The Threat Intelligence Manager is able to explain technical TI subjects to technical experts (i.e. members of the Blue Team) and to non-experts in an understandable manner, delivering actionable threat intelligence for the institution. • Sufficient experience (ideally three years) of the Threat Intelligence Manager in threat intelligence for red team testing. • Intermediate understanding of the workings of the financial sector, its processes, underlying systems, sectoral challenges and threat landscape. • Up-to-date CV to be provided to the entity, specifically in delivering threat intelligence for red team testing activities. • Background checks on the Threat Intelligence Manager are conducted by the TI provider (as a minimum), including those required by the national authorities.

RT provider requirements for ART – for red teaming (replacing table 3 in the TSPG, page 19)

Who	Requirements
RT provider (at company level)	<ul style="list-style-type: none"> For the staff assigned to the test: demonstrably relevant portfolio of comparable previous assignments related to red-team testing. Adequate indemnity insurance in place to cover activities which were not agreed upon in the contract and/or which stem from misconduct, negligence, etc. Capacity to form a core Red Team of three persons, with additional capacity available if needed for specific technologies/situations. No previous or current services delivered for the entity, that would present a conflict of interest for the Service Provider when conducting a TIBER test.
Red Team Test Manager – responsible for the end-to-end management of the TIBER-EU red team test	<ul style="list-style-type: none"> Lead and oversight of the RT provider’s activities for delivering a TIBER-EU test are ensured by a Red Team Test Manager. Sufficient experience of the Red Team Test Manager in red team testing. Expectation: at least three years of experience in red team testing, including one year managing intelligence-led red team tests. The Red Team Test Manager is able to explain advanced, technical RT-subjects to both technical personnel (such as the members of the BT) and to non-experts in an understandable manner, guiding the CT through the RT phase in a clear manner. Intermediate understanding of the workings of the financial sector, its processes, underlying systems, sectoral challenges and threat landscape. Up-to-date CV of the Red Team Test Manager to be provided to the entity, specifically in red team testing activities. Background checks on the Red Team Test Manager by the RT provider (as a minimum), including those required by the national authorities.
Red team (all members of the team, except for the Red Team Test Manager) – responsible for conducting the TIBER-EU red team test	<ul style="list-style-type: none"> Sufficient experience of the Red Team members. Expectation for each member: at least two years of experience in red team testing. Up-to-date CV for each member of the team to be provided to the entity. Multi-disciplinary composition of the Red Team, with a broad range of knowledge and skills, such as: business knowledge, red team testing, penetration testing, reconnaissance, threat intelligence, risk management, exploit development, physical penetration, social engineering, vulnerability analysis and combinations thereof. Basic understanding of the workings of the financial sector, its processes, underlying systems, sectoral challenges and threat landscape. The Red Team members are able to explain advanced, technical RT-subjects to both technical personnel (such as the members of the BT) and to non-experts in an understandable manner, guiding the CT through the RT phase in a clear manner.

- Background checks on each member of the red team are conducted by the RT provider (as a minimum), including those required by the national authorities.
- Ideally, the Red Team should have experience in carrying out intelligence-led red team tests.