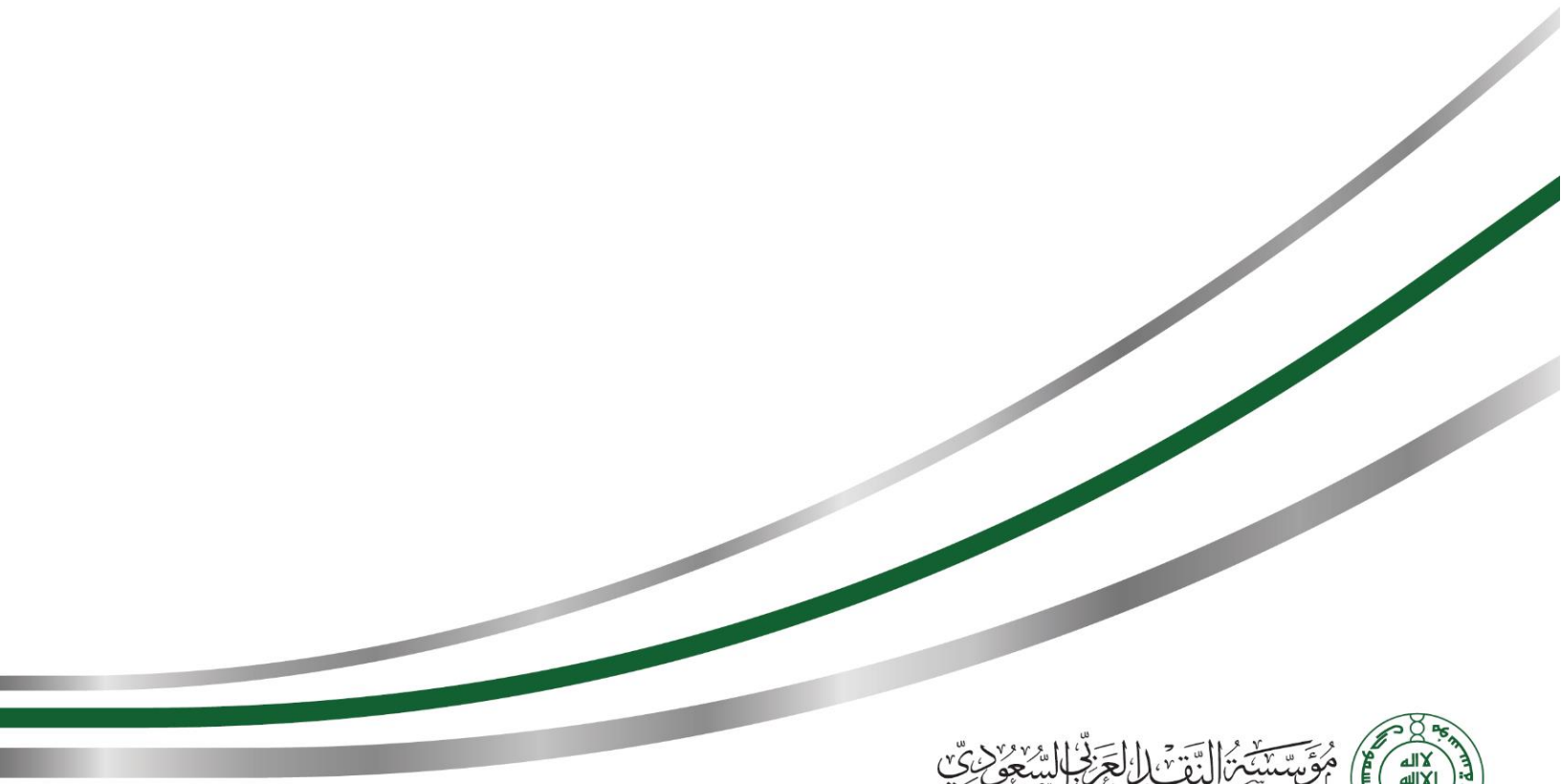
Financial Entities Ethical Red-Teaming

Saudi Arabian Monetary Authority

Version 1.0 May 2019



مؤسسة النقد العربي السعودي
Saudi Arabian Monetary Authority

Contents

1 The Saudi Arabian Financial Entities Ethical Red Teaming Framework

1.1. Introduction

It is crucial that the Member Organizations within the Financial Sector are resilient against the newest and most advanced cyber-attacks.

The Financial Entities Ethical Red Teaming Framework (F.E.E.R.) is intended as a guide for Member Organizations within Saudi Arabia in preparing and executing controlled attacks (i.e. threat intelligence based red teaming tests) against their (live) production environment without exposing sensitive information with the help of certified and experienced Red Teaming Providers.

The Saudi Arabia Monetary Authority (SAMA) has a leading role in the implementation of this Framework. This Framework and associated processes will be continuously improved using the feedback and lessons learned from each red teaming exercise. This framework aims for sharing of intelligence and information obtained during such testing in order to further improve the cyber resilience of the Saudi Arabian Financial Sector.

Red Teaming should not be regarded as an Audit. It is a simulation test, which seeks to provide insight into the level of resilience and effectiveness of the implemented cyber security controls and relevant processes (i.e. detection and response).

Red Teaming is not a penetration test. In contrast to a penetration test (in which one or more specific information assets are tested and assessed), it focuses on replicating a targeted and realistic attack against the entire Member Organization performed in a controlled manner.

The Red Teaming Provider will use the latest attack tactics, techniques and procedures (i.e. TTPs) in an attempt to compromise the Member Organization, aiming to reach the member organizations most important and valuable information assets and to test the detection and response capabilities of the Member Organization. The Red Team consists of certified and experienced ethical hackers with in-depth knowledge of all security domains.

1.2. Objective of the Framework

The principal objective of the framework is to provide guidance on how to conduct the red teaming activities and how to test the detection and response capabilities of the Member Organization against real sophisticated and advanced attacks and enhance the knowledge of the involved stakeholders. Likewise, the Framework aims to support the sharing of threat intelligence and lessons learned with the Member Organizations that will contribute to the cyber resilience of the Saudi Arabian Financial Sector.

The Framework will ensure that the red teaming exercise is executed in a controlled manner. This is important given the nature of the targets during the testing, namely business critical and (live) production systems (i.e. critical information assets).

1.3. Applicability

The Framework applies to all Member Organizations in the Financial Sector regulated by SAMA. SAMA has the authority to select any Member Organization to perform a red teaming exercise considering its criticality and emerging threat landscape. In addition, member organization can rightfully conduct red teaming exercise in order to ensure security resilience.

1.4. Responsibilities

The framework is mandated by SAMA. SAMA is the owner and is responsible for periodically updating the Framework.

1.5. Interpretation

SAMA, as the owner of the Framework, is solely responsible for providing advice on the interpretation of the principles, objectives and considerations, if required.

1.6. Periodicity of the Red Teaming tests

Any Member Organization regulated by SAMA might be selected for red team exercise. However, as minimum, Domestic Systemic important entities will be subject to testing once every three (3) years, in line with this framework.

1.7. Target Audience

The Framework is intended for Senior and Executive Management, business owners, owners of information assets, CISOs and those who are responsible for (or involved in) defining, implementing and reviewing cyber security controls within the Financial Sector and tasked with the improvement of the cyber resilience of the Member Organization.

1.8. Review, Updates and Maintenance

The framework will be maintained by SAMA and reviewed periodically to determine the framework's effectiveness, including the extent to which it addresses emerging cybersecurity threats and risks. If applicable, SAMA will update the Framework based on the outcome of the review and lessons learned.

1.9. Additional Information

For any further information or enquiries about the Saudi Arabian Financial Entities Ethical Red Teaming Framework, please contact IT Risk of Financial Sector Supervision Department.

2 Background

More and more governments, national agencies and regulators consider the protection of their national or sector-wide critical infrastructure as a high priority on their national cyber security agenda. In order to test the cyber resilience of the critical infrastructure, governments, agencies and regulators are increasingly embracing red teaming approaches. These red teaming approaches are generally underpinned by a framework which outlines how red teaming tests should be conducted, how to identify the organizations which should be considered part of the key or core infrastructure and the periodicity or frequency of these tests.

In a red teaming test, an organization performs a 'simulation' of a realistic cyber-attack. The Red Teaming Provider, consisting of certified and experienced ethical hackers, will execute / simulate cyber-attacks based on available threat intelligence and attack scenarios, which aims to test the cyber resilience of an organization.

The cyber security attacks are cautiously modelled and tested, and will simulate a malicious attacker - using their attack approach - from the reconnaissance activities up to the actual compromise of the critical information asset(s). The simulation of these (attack) steps are executed and tested during a red teaming test and will provide vital insights into the organization's resilience against cyber-attacks.

2.1 Stakeholders

The stakeholders within the red teaming exercises have different roles and corresponding responsibilities. Irrespective of role, it is important that everyone is aware that any form of testing is performed in a controlled manner, and that a communication protocol is agreed regarding the sharing of information among the stakeholders. The relevant stakeholders are:

1. SAMA IT Risk of Financial Sector Supervision department – The authority that has primary responsibility for overseeing the Red Teaming exercise.
2. The Member Organization – Each Financial Organization within the Financial Sector of Saudi Arabia and regulated by SAMA.
3. The Security Operations Centre – The SOC positioned within the Member Organization, which will be subject to the red teaming test.
4. The Red Teaming Provider – An external certified party, which has been selected to perform the red teaming exercise and provide required national or sector threat intelligence to define scenarios.
5. Available Member Organization committees (e.g. Banking Committee for Information Security - BCIS) – Relevant results of executed red teaming tests, lessons learned and threat Intelligence might be shared within this committee, in an appropriately sanitized form using the agreed communication protocol, to support the increase of the overall cyber resilience of the (financial) sector.

2.2 Required Teams

For the execution of the red teaming exercise, the following teams should be established:

Green Team

SAMA IT Risk of Financial Sector Supervision department provides the Green Team. The Green Team appoints the Test Manager for each red teaming test. The Test Manager is responsible for guiding and supporting the White Team through the red teaming exercise. The Green Team approves the selection of Red Teaming Provider and provides – when applicable – additional or specific threat intelligence for the Financial Sector.

White Team

Within the Member Organization, the White Team should be appointed (including a White Team Leader), who will be responsible for the controlled execution of the red teaming exercise. The White Team consist of a limited number of security and business experts which are the only staff members that are aware of the red teaming test and who are the single-point-of-contacts (SPOCs), e.g. CISO. They will monitor the test and intervene when needed, e.g. when the test or results of the test are likely to, or have, caused a critical impact, compromise or service disruption.

The overall number of staff members that should be involved in the engagement, should be limited to maximum five (5) people, to avoid a too wide disclosure of the intended cyber-attack simulation and – as a result – that the effectiveness of the exercise is limited or flawed.

Blue Team

The cyber security monitoring team of the Member Organization (e.g. SOC) which monitors and analyses the generated security alerts and events to identify security breaches or flaws. It is the task of the Blue Team to detect the malicious activities (of the Red Team) and to follow the agreed incident response procedures the moment an incident is detected. The Blue Team should never be informed about the test and are expected to follow their standard operating procedures, in order to simulate a realistic attack.

Red Team

The Red Team, a selected third party that executes the attack scenarios and consists of certified and experienced specialists. The Red Team will work with the Green Team and White Team to develop the potential threats and attack scenarios. The Red Teaming Provider is also responsible for providing the latest threat intelligence related to the Financial Sector in order to achieve a certain level of assurance that the Member Organization is tested against the latest known (sophisticated) cyber-attacks.

Please refer to Appendix A – Requirements for Red Teaming Provider, for more details on Red Teaming Provider requirements.

2.3 Penetration Testing versus Red Teaming

There is a significant difference between red teaming exercise and penetration testing. Red teaming focusses on testing the cyber resilience of an organization. In a penetration test, the scope is often limited to an application or system, with the intent to comprehensively test the security of that limited scope application or system.

The overall objective of a red teaming exercise is different from the objective of a penetration test. In a red teaming exercise, the objective is to (independently) test the overall cyber resilience of a Member

Organization. This is achieved by testing the implemented cyber security controls, along with the detection and response capabilities.

A secondary objective is to share the lessons learned with the Member Organizations within the Financial Sector, to further improve the overall cyber resilience within the sector.

Penetration testing	versus	Red Teaming
Gain oversight of vulnerabilities	**Goal**	Test the resilience against realistic attacks
Predefined subset	**Scope**	Realistic access paths
Focus on preventive controls	**Tested controls**	Focus on detection and response
Focus on efficiency	**Test method**	Focus on realistic simulation
Mapping, scanning and exploiting	**Test techniques**	Tactics, Techniques and Procedures (TTPs)
Very limited	**Post-exploitation**	Extensive focus on critical assets or functions
Parts of development lifecycle	**Recurrence**	Periodical exercise

Figure 1 Difference between penetration testing and red teaming

2.4 The Cyber Kill Chain Methodology

The Cyber Kill Chain[1] provides a conceptual model to describe an attack. The term "chain" reflects the end-to-end process adopted by an attacker.

The Cyber Kill Chain provides a good insight into how an attack works and where the different tools and methods employed at each stage. To lower the risk of a successful attack, defensive measures (e.g. preventive, detective and responsive and corrective) should be considered and taken for each of the steps of the kill chain to reduce the probability of being compromised and improve the resilience of the Member Organization.

The following seven (7) stages characterize an advanced cyber-attack in the cyber kill chain:

Figure 2 Seven stages of a cyber-attack, with the red team and blue teams main tasks

1. Reconnaissance:

The first stage is about selecting a target and gathering information about the target to determine attack methods. This happens before the attack is executed. Examples of useful information can be: names,

[1] Computer scientists at Lockheed-Martin corporation developed and described the "intrusion kill chain" framework to defend computer networks in 2011.

phone numbers, email addresses, functions, private or professional areas of interest of employees on the internet and published information about the software that an organization is using.

2. Weaponize:

The attacker creates the malicious payload/file for a specific target based upon information retrieved during the reconnaissance stage. The attack can come in many different formats and is based upon the creativity of the attacker, the available set of defenses and the possible vulnerabilities.

3. Delivery:

The transmission of the crafted attack to the victims by the use of different means, such as: email (attachments), phishing, websites, physical devices or social engineering.

4. Exploitation:

Triggering or activating the malicious payload/file (i.e. malware) will result in a successful penetration of the target's system and network. A staged malware attack limits the possibility of detection. The malware will communicate back to the malicious attacker over a secure channel, which limits the chance of detection. Attackers usually use popular methods and file formats to deliver the malware executables (e.g. Microsoft office files, pdf files, malicious websites, phishing emails and removable media).

5. Installation:

The actual installation of malicious payload/file or software that supports the malicious attacker. In order to make the malware and backdoor(s) persistent, the attackers could install additional malware or malicious software tools to ensure that the attack can continue if the initial compromised system or active malware is disabled.

6. Command and Control:

A compromised system will usually connect back to the attacker, to establish a so-called command-and-control channel, which allows remote control of the malware. Especially in advanced persistent threat (APT) malware, the attacker will control the malware and explore the network by using this type of remote access.

7. Actions on Objective:

After the attacker completed his malicious actions or achieved his goals, the attacker will try to cover his digital tracks and traces by using different techniques, like data exfiltration, or will use the compromised system as starting point to 'hop on' to other systems in the network (i.e. *lateral movement),* to search for other high value assets or targets.

2.5 Threat intelligence

The Red Teaming Provider(s) will maintain and deliver the threat intelligence landscape relevant for Saudi Arabian Financial Sector or specific Member Organization. This can be enriched using the provided input from SAMA (i.e. the IT Risk of Financial Sector Supervision department, or the Green Team), the White Team and, various governmental agencies. The Red Teaming Providers should provide the latest threat intelligence related to the Financial Sector in order to achieve a certain level of assurance that the Member Organization is tested against the latest known (sophisticated) cyber-attacks.

2.6 Overview of the Phases

The Saudi Arabian Financial Entities Ethical Red Teaming Framework consists of four phases. In the corresponding chapters of this framework, each phase is described in detail.

Please refer to Appendix C – Glossary for more details and definitions regarding this Framework.

3 Preparation phase

3.1 Overview

The Green Team initiates the preparation phase of the red teaming exercise by appointing a Test Manager. A Backup Test Manager should also be nominated given the importance of this role.

The Test Manager is responsible for contacting the Member Organization to explain the red teaming concept and processes. The Test Manager will invite the Member Organization to appoint and formalize their White Team and start contracting the Red Teaming Provider.

The White Team Leader initiates a kick-off session, where all relevant stakeholders (i.e. Green, White and Red Team) are invited to align the ambition and objectives of the red teaming exercise.

3.2 Green Team: Determining Test Manager

The Test Manager is a crucial person during the Red Teaming exercise. This person should have extensive experience in project management and in-depth understanding of the banking and cyber security sector.

The Test Manager of the Green Team should invite the Member Organization to appoint a White Team. During the entire red teaming exercise, the White Team will keep close contact with the Test Manager.

The Test Manager will oversee the Red Teaming exercise and will provide support, guidance and reflections to ensure that the entire Red Teaming exercise performed by the White Team and Red Teaming Provider is in line with the Framework. As the Test Manager is not a formal part of the White Team, he cannot be held accountable for any actions or consequences.

3.3 Selecting a Red Teaming Provider

The Green Team will appoint the red team provider, who are pre-selected to execute the Red Teaming tests, based on their experiences and skilled staff. Given the fact, that these ethical hacking tests are carried out on the live production systems, it is crucial that the Red Teaming Provider has a proven track record and has the required skills, expertise, certifications and experienced staff to perform the red teaming test.

Please refer to Appendix A – Requirements for Red Teaming Provider, for more details on Red Teaming Provider requirements.

3.4 Determining White Team

The Member Organization should carefully establish a White Team and nominate a White Team Leader in order to facilitate, oversee and lead the red teaming exercises during all phases. The White Team Leader's role is to make sure that the entire Red Teaming exercise is performed in a controlled manner, on behalf of the Member Organization. After establishing the White Team, the White Team Leader needs to coordinate with the appointed Red Teaming Provider for contract and invite the Red Teaming Provider to the kick-off meeting.

3.5 Procuring a Red Teaming Provider

Upon approval of the Red Teaming Provider by the Green Team, the Member Organization should initiate their procurement process. During the procurement of the Red Teaming Provider, the Member Organization should undertake the following activities:

- Agreeing on contractual considerations, e.g. Non-Disclosure Agreement (NDA) clauses, the liability for any consequence flowing from the test, and a Letter of Authorization (LOA);
- Introduce the Red Team members to the White and Green Team.

Please refer to Appendix A – Requirements for Red Teaming Provider, for more details on Red Teaming Provider requirements.

After the procurement of the Red Teaming Provider, the White Team should start involving the Red Teaming Provider and its identified staff, to ensure their experience and input is fully utilized and that the staff of the Red Teaming Provider is introduced into the business model and services of the Member Organization.

3.6 Defining the Scope

During a kick-off session with all relevant stakeholders (Green, White and Red Team), the scope and the target critical information assets (i.e. 'red flags') should be defined for the attack scenarios. Moreover, the planning of the project is discussed in detail along with the responsibilities for each team. Deliverables and contractual considerations should be discussed during the session. The White Team should determine the flags that should be targeted or attacked.

The Red Teaming Provider will share their advice and recommendations to the White and Green Team based on their (previous) experience in order to support the scoping discussion.

Boundaries, limitations and escalation procedure for the red teaming test should be discussed and defined by the White Team with mutual understanding with the Green Team. Another important step is to agree on the liability for the actions of the Red Teaming Provider (see also 3.5).

The White Team should create a Scoping document. This document should contain contact details of the White Team members and the identified flags (i.e. defined goals or target systems) during the red teaming exercise. This document also contains the overall plan for the exercise, predefined escalation procedures and communication protocols (including the code-name for the test).

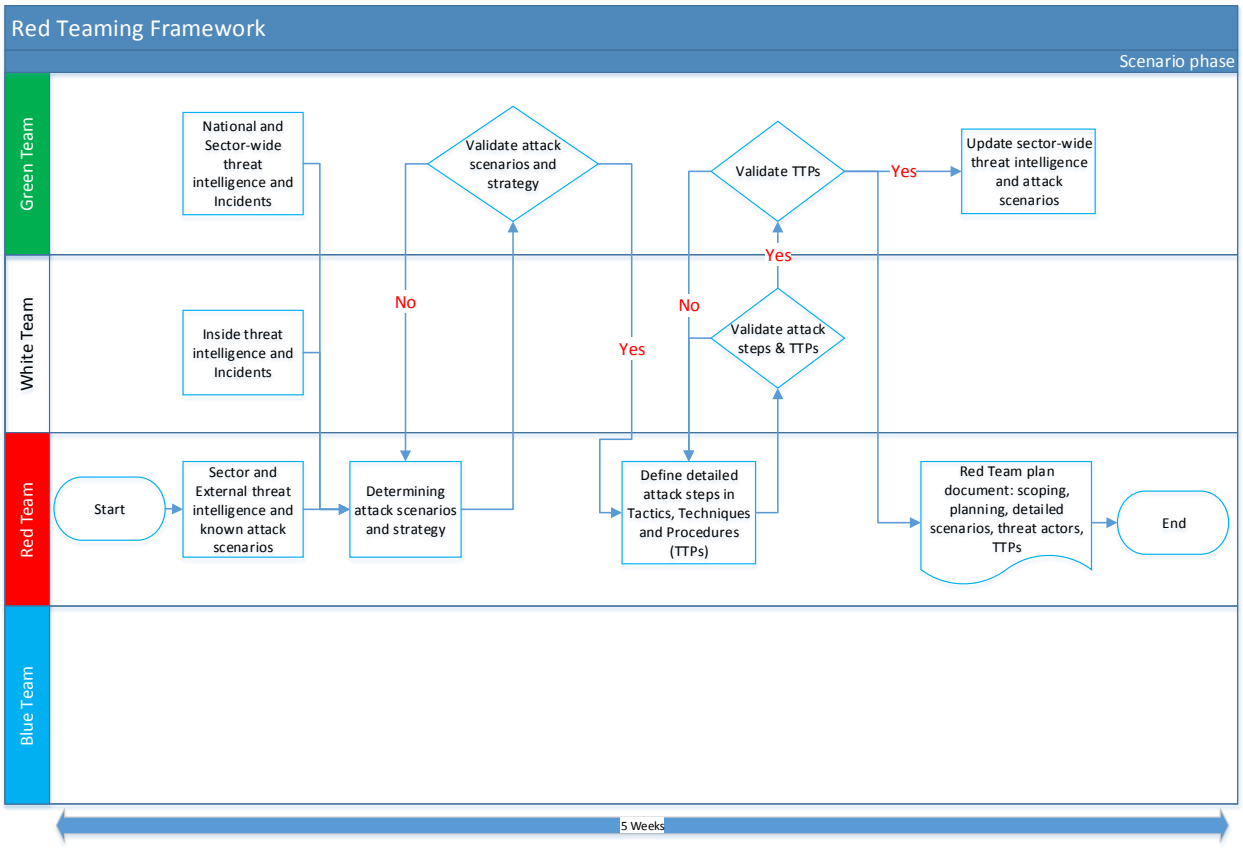
Once the scope is defined by the White Team, the Scoping document should be submitted to the Green Team for approval.

4 Scenario phase

4.1 Overview

At the beginning of this phase, the Green and White Team should independently provide their available Threat Intelligence (TI) to the Red Team. The Red Teaming provider will combine the received Threat Intelligence, with their own Threat Intelligence (which should be based on their own sources, their experience and earlier executed tests). Based on the combined threat intelligence the Red Team determines the attack scenarios and strategies. These attack scenarios and strategies are than discussed with the Green Team before defining the detailed attack Tactics, Techniques and Procedures (TTPs). If necessary, a discussion with Red and White Team should be initiated to further discuss and agree on the final attack scenarios in the light of Green Team comments.

The scenario phase usually takes several weeks (maximal five (5) weeks). An overview of the process is depicted below:



4.2 Threat Intelligence Gathering

Each of the teams provides their collated threat Intelligence independently. The Green Team will provide (when available) their sector-wide threat intelligence which is known and available via the Member Organizations or incidents. This may include threat intelligence from governmental agencies, which could be relevant to the Member Organization. The White Team should provide the Member Organization's input including specific threat intelligence considered relevant for their business and linked to the internal or external trends or incidents, they identified.

The Red Teaming Provider will combine the received threat intelligence with their external threat intelligence (including and using their own 'open' sources), and the intelligence gathered during various red teaming engagements.

4.3 Defining and Approval of high-level attack scenarios

Based on all received threat intelligence, the Red Team should analyze, outline and create realistic attack scenarios and prepare a test strategy document. Once the scenarios are determined, the attack scenarios and test strategy should be agreed upon before the Red Teaming Provider starts with the creation of the specific attack scenarios.

4.4 Preparing and Approval of detailed attack scenarios

The detailed attack scenarios should be mapped to one or more critical information assets combining the external, internal (i.e. Member Organization specific) and sector-wide threat intelligence. Each attack scenario should include a written description of the kill chain from the attacker's point of view. The Red Teaming Provider should indicate various attack options, based on various tactics, techniques and procedures (TTPs) used by experienced testers and attackers. As with the high-level attack scenarios and test strategy, the detailed scenarios have to be agreed with the Green Team.

4.5 Finalizing the Red Teaming Plan

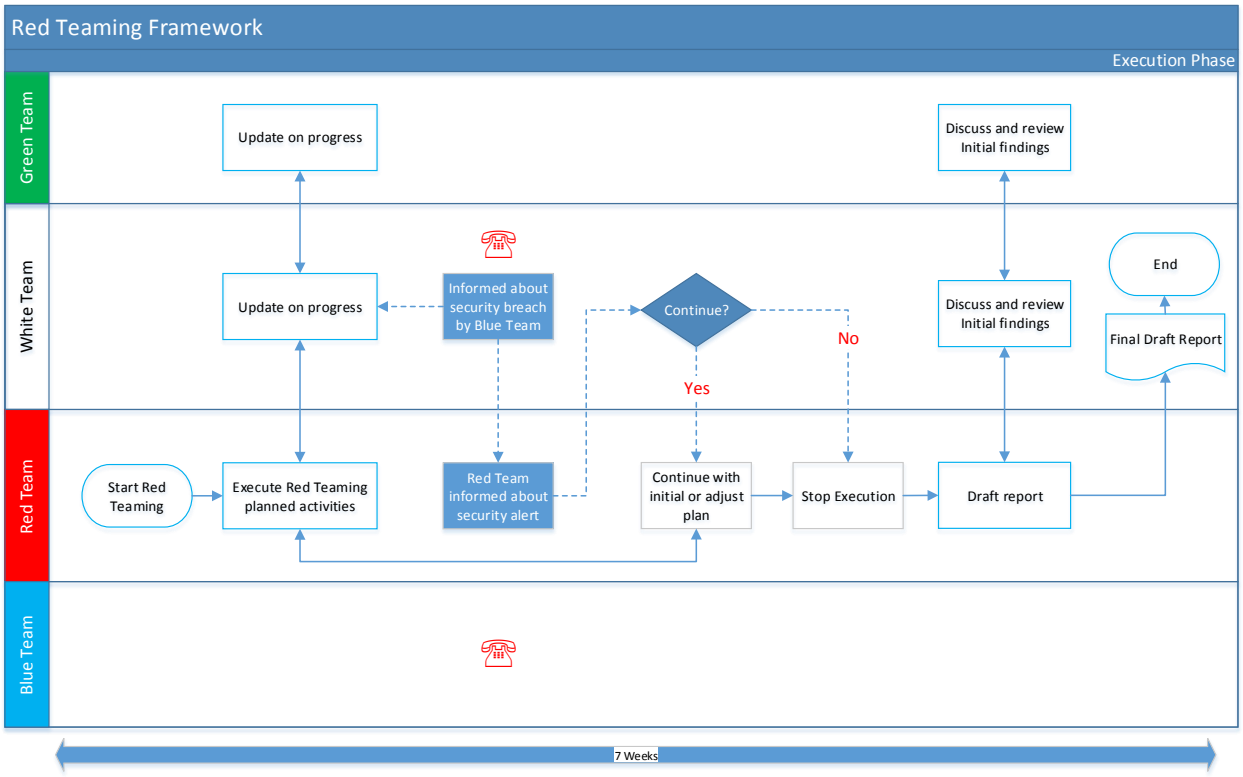
The final red teaming plan should not only consist of the different attack scenarios that the Red Teaming Provider will perform, but also define the agreed escalation procedures and communication protocols. Given the fact that critical production systems are in scope for the red teaming test, the Red Teaming Provider should be aware and consider how to react in case of any unexpected issues or disruptions. After finalizing the red teaming plan, final approval by the White and Green Team is required before Red Teaming Provider can proceed with executing the attack scenarios.

5 Execution phase

5.1 Overview

The phase starts with the Red Teaming Provider executing the attack scenarios. During the process, the White and Green Team should be updated regularly. All actions should be logged for evidence and replay purposes, with the Blue Team.

An overview of the process is depicted below:



5.2 Execute Red Teaming plan

The Red Teaming Provider should start the execution of the red teaming exercise following the agreed scenarios and against the identified critical (information) assets or functions. It should be noted that the agreed scenarios do not have to be followed precisely as these are outline and may not reflect the precise operational environment encountered during the execution phase. Nevertheless, the Red Teaming Provider should inform the White Team Leader and Green Team about the suggested adjustments in the scenarios. Deviation from the initial scenarios should be allowed and is desirable if obstacles are encountered.

Red Teaming Provider should apply their expertise and 'creativity' to develop alternative ways or workarounds in order to reach the identified critical (information) assets or functions. It is crucial that the Red Teaming Provider remains in close contact with both the Green and the White Team and does provide periodic updates on the progress made during the red teaming test - in line with the frequency which was agreed during the kick-off, or in case of escalations or severe incidents or occurrences - immediately.

5.3 Executing the Defined and Agreed Scenarios

If the Blue Team detects any events triggered by the Red Team while performing their actions, the Red Teaming Provider should decide in conjunction with the White Team Leader if the red teaming test can be continued in line with the initial plan or whether the initial attack plan can be adjusted.

The White Team Leader should consider the following options when the actions of the Red Teaming Provider are detected:

1. Stop or postpone the test in case there is a significant risk of a business disruption;
2. Carefully monitor and direct the Blue Team or response activities, in case extreme actions are about to be taken (i.e. reporting the incident to law enforcement, shutting down critical services to avoid to avoid further impact from the incident, ..Etc.);
3. Inform the Red Teaming Provider to continue with the initial attack scenarios;
4. Inform the Red Teaming Provider to revise the (detected) attack or to create a workaround for the specific critical information asset and continue with the revised attack scenario after approval from the White Team Leader;
5. Inform Green Team on the detection of events and decision on the exercise.
6. Request the Red Teaming Provider to re-engineer an alternate attack scenario for an adjusted critical information assets (e.g. change in scope).

5.4 Reporting

After completing the red teaming test, or stopping upon request of the White Team Leader, the Red Teaming Provider should prepare their initial observations and findings, preferably in chronological order. These observations and results should be discussed with the Green and White Team. These observations and findings provide the basis of evaluating the detection and response capabilities of the Blue Team. After the preliminary evaluation, the White Team should share their observations, from their respective role and point of view.

Note. After completing the red teaming test the Red Teaming Provider is required to immediately inform the White Team Leader of the installed red teaming scripts, code or malware, etc., including an overview the user-ids which were created, compromised or (re)used during the test. The White Team Leader needs to evidence to the Green Team that these 'indicators of compromise' were removed or reset.

The White Team should include insights of what has and has not been detected or observed by the Blue Team. The Red Teaming Provider should use this information to overall assess and evaluate the Blue Team's detection and response capabilities in the draft report. The Red Teaming Provider should include all relevant observations, findings, recommendations and evaluations, which were noted or experienced during preparation, scenario and execution phase, including those from the White and Green Team. The provided recommendation should consider SAMA Cyber Security Framework and other applicable industry good practice.

The final report should include the exploited cyber kill chains, summarized in the form of attack vector diagrams. These attack vector diagrams should provide insights into how the attack scenarios were executed and where to focus on when implementing mitigating controls. The final report should be agreed upon by all Teams involved and copy of the report should be submitted to SAMA by the provider.

Please refer to Appendix B – Requirements for Reporting, for more details on Red Teaming Provider requirements.

6 Lessons Learned phase

6.1 Overview

In this phase, the Red Teaming Provider should deliver the final red teaming report, which should contain the overall assessment of the Member Organization's resilience against targeted cyber-attacks.

The Blue Team should deliver the blue team report with their observations, findings and recommendations and should focus on the alerts and actions taken as part of the detection and response capabilities of the Member Organization.

Once the final red and blue team reports are distributed to all Teams. The White Team should invite the Red, Blue and Green Teams to participate in a (360 degrees) feedback session in which they share their observations and experiences for learning purposes (of the staff and management involved), to understand what capabilities need to be improved (e.g. prevent, detect and respond) and (enhancing) future exercises.

After the feedback session, a Replay Exercise should be organized, led by the Blue and Red Team. The objective of the joint Replay Exercise is to step through the red team exercise, discussing all the relevant actions and observations, highlighted from both angles, i.e. the Blue and Red Team.

The next step is the overall evaluation of the red teaming exercise processes itself. The outcome of the evaluation may contribute to vital information to enhance the Financial Entities Ethical Red Teaming Framework for future exercises.

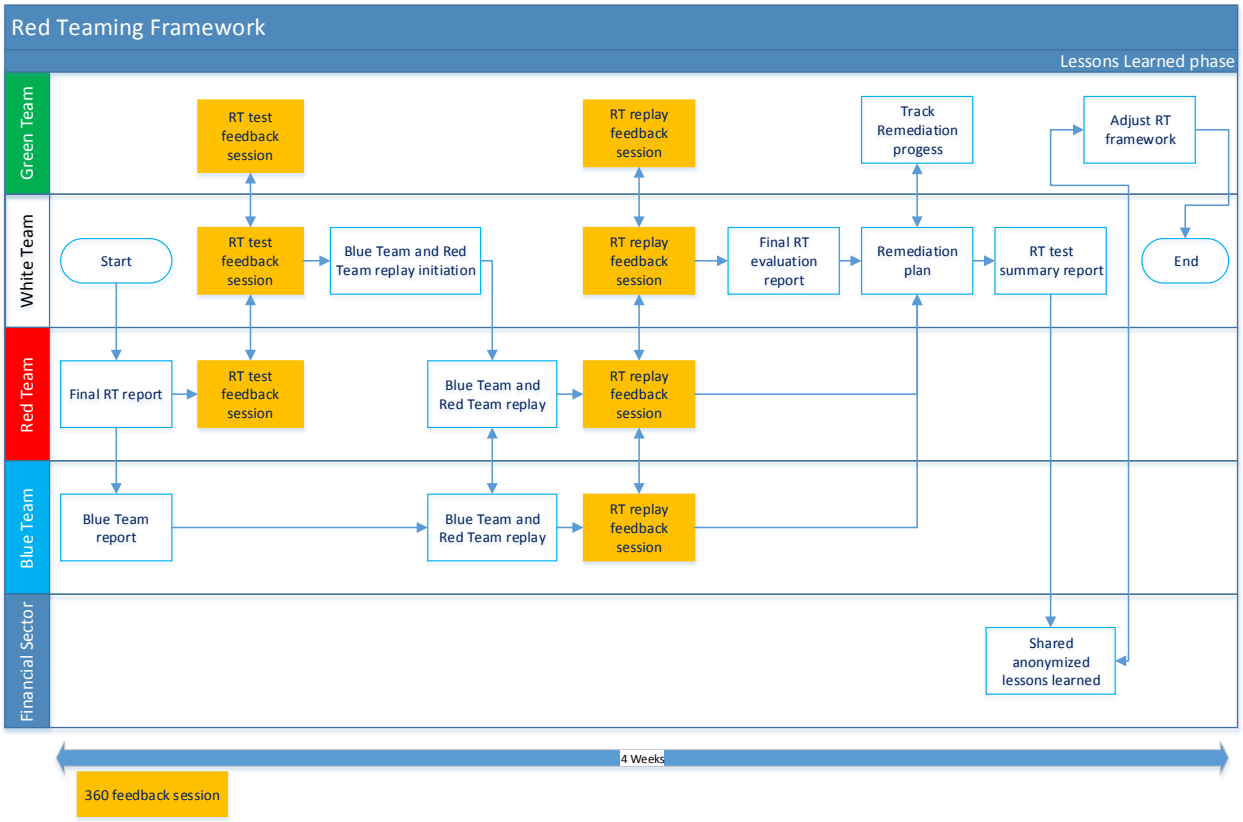
The White Team should create a remediation plan based on the detailed observations and recommendations.

To ensure that all Member Organizations within the Financial Sector benefit from these red teaming exercises, an anonymized summary report of the executed red teaming test should be provided, and if required presented. The sharing of this report should be limited to the agreed with the closed community (i.e. addresses) and within the boundaries of the agreed communication protocol.

The duration of this phase is approximately four (4) weeks.

Based on the evaluations, feedback and sharing sessions SAMA should review, discuss and initiate adjustments to improve the current Framework, if required.

An overview of the Lessons Learned process is depicted below:



6.2 Debriefing

The Red Teaming Provider finalizes the red teaming report and presents the output to all the White and Blue Team. Simultaneously, the Blue Team should create a blue team report. The blue team report should provide the observations from the perspective of the Blue Team and should include the alert and events detected; the actions initiated and the result of these actions. The blue team reports should also provide the Blue Team's recommendations for improvements.

It is important that all teams (i.e. Green, White and Red) that were directly involved in the red teaming test provide their (360 degrees) feedback on the executed red teaming test. The White Team should initiate and schedule a joint replay session with all the teams.

6.3 Red and Blue Team Replay Exercise

After delivering the red and blue team reports, the White Team should organize a Replay Exercise. During this Replay Exercise, the Blue and Red Team jointly perform a chronological walkthrough of the red teaming exercise and the relevant alerts, events and attack steps that were initiated.

The purpose of the Replay Exercise is to explain and discuss each step and action individually to assess whether the alert or detected event lead to the expected actions. It is important to determine whether the initiated actions led to the expected results and whether the actions were correctly initiated or should be subject for improvement.

Replaying the red teaming exercise should ensure the more comprehensive (in-depth) understanding of the performed attack patterns, the current maturity of the detection and response capabilities and the implemented layered defenses or controls within the tested Member Organization.

Additionally, the White Team may repeat the replay exercise for specific target audiences within the Member Organization. It is strongly suggested to re-perform the replay exercise for:

a. The relevant staff members within the IT organization – the scope of this session can be a very in-depth and technical session in order to provide the relevant insights in the technical and procedural aspects.

> *Note. When the level of detail is insufficient or the attack steps cannot be demonstrated, then there can be a tendency for members within the IT organization to downplay these attacks or argue that the exercise is just theoritical.*

b. The Senior Management – a high-level replay session with the Senior Management should also seek to raise awareness and educate Senior Management. The replay session should provide an overview and objective of the red teaming exercise, an overview of the performed attacks and responses, an overview of the current detection capabilities and an overview of the suggested improvements required to further improve the cyber resilience.

6.4 Defining the Remediation Plan

The White Team should create a remediation plan based on the recommendations provided by the Red Team and Blue Team. The White Team should:

- analyze the observations and recommendations;
- determine the improvements regarding the detection and response capabilities;
- determine the associated risks and priorities.

The White Team shares the internally agreed and approved remediation plan with the Green Team and periodically track the remediation progress to ensure that the vulnerabilities identified are monitored and mitigated.

> *Note: The Green Team should not actively share nor distribute the red and blue team reports, nor the evaluation reports, nor the remediation plan unless the Member Organization provides written permission.*
>
> *As stated earlier, the primary objective of this Framework is exercising, learning and sharing.*

6.5 Remediate Identified Vulnerabilities

Shortly after finishing the red teaming exercise, the Member Organization, i.e. the White Team should start executing the agreed remediation activities and address the identified vulnerabilities.

The Member Organization should be tracking the actual remediation progress to ensure the timely execution and delivery of the improved capabilities. The Member Organization should ensure that the Cyber Security Committee (and if required the Senior Management) is periodically updated on the

progress of the planned remediation actions, and should request support when remediation activities do not progress as expected.

6.6 Sharing of the Lesson Learned

An important activity within the lesson-learned phase is to provide an anonymized summary report of the executed red teaming test, which might be shared with Members Organizations Committees like e.g. BCIS.

Sharing the summarized report and the lessons learned helps other Member Organizations build the knowledge and experience they need to improve their own cyber resilience.

Note. The sharing of the report and lessons learned should be limited to the agreed with the closed community (i.e. addresses) and within the boundaries of the agreed communication protocol.

By applying the lessons learned within their own Member Organizations the cyber resilience of the overall Saudi Arabian Financial Sector will improve, regardless of whether the Member Organizations are considered systematic for the sector, or not.

6.7 Enhancing the Red Teaming Framework

Based on the evaluations, feedback and lessons learned sharing sessions SAMA should review, discuss and initiate adjustments to improve the current Framework for future red teaming exercises.

Appendix A – Requirements for Red Teaming Provider

The following requirements should be considered when selecting and procuring a Red Teaming Provider.

Proven Red Teaming Experience and References
1. The Red Teaming Provider should be able to show evidence of a solid reputation, history and business / professional ethics (e.g. a good business history, good feedback from both clients and providers, a reliable financial record and a strong history of performance); 2. The number of credentials and references (i.e. large organizations) of successfully executed red teaming tests; 3. The Red Teaming Provider should be able to show independent feedback on the quality of work performed and conduct of staff involved (internal accreditation); 4. The Red Teaming Provider should be able to provide (anonymized) reports of earlier tests, preferably in the same or similar field of work and similar tests; 5. The Red Teaming Provider should be able to demonstrate exploits or vulnerabilities found in other similar environments; 6. The Red Teaming Provider should demonstrate and proof the certification and experience of the staff involved in the red teaming test(s) – see table below for more details; 7. The Red Teaming Provider should have taken part in specialized industry events (such as those run by BlackHat or RSA Conference etc.) – this is optional but should be considered as an additional reference and experience.

1. The Red Teaming Provider should have a clearly defined process in place for red teaming tests and the related operations; these should describe the activities regarding: the preparation, scenario development, execution and lessons learned phases activities and requirements; 2. Key element in Red Teaming Provider's approach should be the learning experience for the Blue Team and feedback session to improve the knowledge of the involved staff and departments and to mature the cyber security detection, response and recover processes and control measures and where required the prevention measures (e.g. security hardening); 3. The Red Teaming Provider should be able to assist in creating and maintaining a knowledge base so that known weaknesses and lessons learned can be shared and improved within the Financial Sector; 4. The Red Teaming Provider should have a verifiable quality assurance and escalation structure in place for their red teaming operations; 5. All activities from the Red Teaming Provider should be reproducible (e.g. logging all activities); 6. The Red Teaming Provider should adhere to a formal code of conduct overseen by an internal/external party; 7. The Red Teaming Provider should be able to proof that it provides high quality services, including the methodologies, tools, techniques and sources of information that will be used as part of the red teaming and testing process; 8. The Red Teaming Provider should be able to proof that results of tests are generated, reported, stored, communicated and destroyed in a way that does not put a Member Organization at risk;

9. The Red Teaming Provider should ensure that no data leakage occurs from the testers laptops and systems and that all data obtained is securely stored during and securely destroyed after the engagement;
10. Any (agreed) data exfiltration by the Red Teaming provider should be restricted to the extent just required to prove the attack scenario. This data should only be stored in encrypted format and locally (not at cloud providers).
11. The Red Teaming Provider should assure the privacy of the staff within the Member Organization;
12. The Red Teaming Provider should be able to provide a written assurance that the activities and risks associated with the red teaming test and that confidential information will be adequately addressed and performed in line with the security and compliance requirements of the Member Organization;
13. A Letter of Authorization including non-disclosure terms should be mutually agreed between the Red Teaming Provider and the White Team to ensure that potential liability or legal issues are covered.

The Red Teaming Provider should consider the one or more of the following suggested certifications for its managers and testers, which will participate in the red teaming exercise. Verification of the certification of the staff and level of practical experience is key when selecting or procuring the Red Teaming Provider.

Recommended Certification(s) for the Red Teaming Provider's Staff		
Role	**Institute**	**Certification**
Managers	ISACA	• Certified Information Systems Auditor (CISA) • Certified Information Security Manager (CISM) • Cybersecurity Nexus (CSX)
	(ISC)2	• Certified Information Systems Security Professional (CISSP) • Systems Security Certified Practitioner (SSCP)
	CREST	• CREST Certified Simulated Attack Manager (CCSAM) • CREST Certified Threat Intelligence Manager (CC TIM) – Optional
Testers	SAN Institute – GIAC	• GIAC Penetration Tester (GPEN) • GIAC Web Application Penetration Tester (GWART) • GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
	Offensive Security	• Offensive Security Certified Professional (OSCP) • Offensive Security Wireless Professional (OSWP) • Offensive Security Certified Expert (OSCE) • Offensive Security Exploitation Expert (OSEE) • Offensive Security Web Expert (OSWE)
	CREST	• CREST Certified Simulated Attack Specialist (CCSAS) • CREST Registered Threat Intelligence Analyst (CRTIA) - Optional

Appendix B – Requirements for Reporting

The following content should be considered when drafting the reports and providing the deliverables.

Note. All reports should only be provided via secure communication channels and shared under an agreed communication protocol (i.e. need-to-have and for-you-eyes-only).

Red Team Evaluation Report (RTER)

At the end of the red teaming exercise, the Red Teaming Provider will draft an evaluation test report, which contains an assessment of the Member Organization's cyber security resilience against the executed cyber security attacks. The report should include a diagram of how the attack scenarios were executed. This report should be issued to the White Team, Blue Team and Green Team.

Below the outline of the report and the required elements (not limitative):

Red Team Evaluation Report (RTER)

1. Introduction
2. Executive summary
3. Scope
   - Scope of the agreed red teaming test
   - Background on the agreed targeted critical (information) assets and functions
   - Goal and objectives of the red teaming test
   - Items which were explicitly out-of-scope
4. Control Framework - references
   - F.E.E.R. Framework
   - OWASP (Top-10)
   - Others
5. Execution Methodology
   - Listing all the attack stages and actions performed by the Red Team during the red teaming test
   - How the each attack scenario was conducted, how, when and where (i.e. the exploited cyber kill chains, summarized in the form of attack vector diagrams)
   - Explanation of the Cyber Kill Chain methodology and Tactics, Techniques and Procedures that were planned and eventually executed
   - The timeline of activities performed (dates and time)
   - What specific tools or software and methods were used during the attack scenarios
   - Methodology for the risk rating for the observations
6. Observations
   - Listing of the identified vulnerabilities and the weaknesses of events that did occur
   - Observations focused on people, process and technology
   - Observations focused on detection, response and recover
   - Suggested risk description and risk rating for each observations
   - Recommendations on suggested improvements
7. Conclusions

- An overall conclusion of the cyber resilience of the Member Organization
- Detailed conclusions for each attack scenario performed
- A conclusion per agreed critical information assets or function

Appendices

- The list of involved teams and team members
- Screenshots with evidence
- Any other supportive materials

The report should be classified as: Confidential

Blue Team Report (BTR)

After the distribution of the Red Team Evaluation Report, the Blue Team will generate their own report. This report should be based on the monitoring and detection alerts, response and recover activities and process-steps taken by the Blue Team during the exercise. The report should include the defense and monitoring techniques and capabilities that the Blue Team is currently using to detect cyber security attacks (e.g. events, alerts, incidents). The report should also include the Blue Team's observations regarding the identified limitations or weaknesses.

Below the outline of the report and the required elements (not limitative):

Blue Team Report (BTR)
1. Introduction 2. Executive summary 3. Background of the report • Goal and objectives of the red teaming test 4. Introduction into the financial sector current threat landscape and cyber-attack trends 5. Explanation of the current incident handling, incident response and crisis management processes regarding cyber incidents within the Member Organization • Process flows • People/teams involved • Overview of the relevant tasks and responsibilities 6. Time line of the detected activities or generated alerts (against the performed red teaming exercise and activities) 7. Observations per performed attack scenario (chronological) • First notification(s) or alert(s) • The monitoring and defense tools and techniques used • Incident response plan and steps performed (e.g. was the crisis management organization activated and what where the observations) • Involvement of other departments (e.g. Help desk, CISO, CIO, HR, Legal, Public Relations) • What where the results reported by the Red Team • What went well or what can or should be improved • Results of the root-cause analysis performed 8. Recommendations or areas of improvement

- Recommendations focused on people, process and technology,
- Recommendations focused on detection, response and recover
- Suggested priority rating for each recommendation
- Roadmap for the suggested improvements
- Suggested input for upcoming cyber security awareness campaigns

9. Conclusions
    - An overall conclusion of the current cyber resilience state of the Member Organization
    - The conclusions regarding the required and suggested improvements (from both the Blue and Red Team)
    - Detailed conclusions for each attack scenario performed and the state of the current capabilities of the Blue Team

Appendices

- The list of involved departments, teams and team members
- Screenshots with supporting evidence
- Any other supportive materials

The report should be classified as: Confidential

Remediation Plan (RP)

The White Team should draft a Remediation Plan, which should be based on the Red Teaming Evaluation Report and the Blue Team Report. The remediation plan should provide clear areas of improvements, priorities and a roadmap how and when to improve the prevention (e.g. hardening), detection, response and recover capabilities within the Member Organization. Important is that the status and progress of the remediation plan is monitored and periodically reported to the Cyber Security Committee of the Member Organization as well as the Green Team.

Below the outline of the report and the required elements (not limitative):

Remediation Plan (RP)

1. Introduction
2. Executive summary
3. Background of the remediation plan
    - Goal and objectives of the remediation plan
4. Target audience and stakeholders
5. Agreed recommendations and areas of improvement provided by the Red and Blue Team
    - Agreed recommendations focused on people, process and technology,
    - Agreed recommendations focused on (prevention) detection, response and recover
    - Agreed priority rating for each recommendation
6. Prioritized list of the agreed areas of improvement
7. Agreed Remediation Plan
    - What, when, where, and how
    - Overview of the persons-to-act (e.g. where possible involvement business management)
    - Agreed due dates

8. Roadmap for the agreed and prioritized improvements
9. Frequency of updating the Cyber Security Committee of the Member Organization and the Green Team
10. Project Management Organization
    - People/teams involved
    - Overview of the relevant tasks and responsibilities

Appendices

- The list of involved departments, teams and team members
- Screenshots with supporting evidence
- Any other supportive materials

The remediation plan should be classified as: Confidential / Internal Use Only

Red Teaming Test Summary Report (RTTSR)

When the Remediation Plan is finalized, the White team will generate a summary test report (fully anonymized) in order to share via SAMA (i.e. the Green Team Test Manager) to all relevant Member Organization Committees (e.g. the BCIS). The summary test report should cover the current threat landscape for the financial sector, the red teaming test results and the observed weaknesses or vulnerabilities during the red teaming test and should include the lessons learned.

This report should only be provided via a secure communication channels and shared under an agreed communication protocol (i.e. need-to-have and for-you-eyes-only).

Below the outline of the report and the required elements (not limitative):

Red Teaming Test Summary Report (RTTSR)

1. Introduction
2. Personalized distribution list (to ensure the agreed communication protocol)
3. Executive summary
4. Background of the executed red teaming test
5. The financial sector current threat landscape and recent cyber-attack trends
6. The outline of each attack scenarios executed
    - Listing of the most relevant identified vulnerabilities and weaknesses
    - Most relevant observations focused on people, process and technology
    - Most relevant observations focused on detection, response and recover
7. Lessons learned
8. Suggestions for the Financial Sector
9. Recommendations for adjusting the Saudi Arabian Financial Entities Ethical Red Teaming Framework

The Red Teaming Test Summary plan should be classified: Highly Confidential (need-to-have and for-you-eyes-only)

Appendix C - Glossary

Term	**Description**
Resilience	The ability to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.
Cyber-attacks	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. Ref (NIST SP 800-39 (CNSSI 4009))
MO	Member Organization - Organizations affiliated with SAMA.
F.E.E.R.	The Financial Entities Ethical Red Teaming Framework
KSA	Kingdom of Saudi Arabia
Red Teaming	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.
SAMA	Saudi Arabian Monetary Authority
Penetration test	Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. Ref (NIST SP 800-115)
TTPs	Tactics, Techniques and Procedures
Ethical hackers	An expert, performing a penetration test. Refer to 'Penetration test'.
LoA	Letter of Authorization
BCIS	The Banking Committee for Information Security
CISO	Chief information security officer (CISO). A senior-level executive responsible for establishing and maintaining the enterprise cyber security vision, strategy, and program to ensure information assets and technologies are adequately protected.
Social Engineering	A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. Ref: (NIST SP 800-114)

Blue Team	A group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cybersecurity readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems. Ref: (CNSSI 4009-2015)
SOC	A security operations center (SOC) is a specialized location (and team) where security-related data from enterprise information systems (e.g., web sites, applications, databases, servers, networks, desktops and other devices) is monitored, assessed and actioned. The SOC is often dedicated to the detection, investigation and potential response to indicators of compromise. The SOC works closely with, and disseminates, collated security-related information to other areas of the organization (e.g., the cyber security function, incident management team and IT service owners).
Cyber kill chain	Contractual concept used to structure a cyber-attack.
White Team	The group responsible for referring an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of their enterprise's use of information systems. In an exercise, the White Team acts as the judges, enforces the rules of the exercise, observes the exercise, scores teams, resolves any problems that may arise, handles all requests for information or questions, and ensures that the competition runs fairly and does not cause operational problems for the defender's mission. The White Team helps to establish the rules of engagement, the metrics for assessing results and the procedures for providing operational security for the engagement. The White Team normally has responsibility for deriving lessons-learned, conducting the post engagement assessment, and promulgating results. Ref: (CNSSI 4009-2015)
Green Team	The Green Team is provided by the SAMA Financial Sector Cyber Team. The Green Team appoints the Test Manager for each red teaming test. The Green Team also maintains a short list of potential Red Teaming Providers and provides the threat intelligence for the Financial Sector.
Test Manager	The Test Manager is responsible for a guiding the White Team through the red teaming exercise.
Risk	A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (NISTIR 7298r2 Glossary of Key Information Security Terms)
Exploit	A piece of code or a command, which purposes to perform malicious activities on a system, by taking advantage of a vulnerability.

Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NISTIR 7298r2 Glossary of Key Information Security Terms)
NDA	Non-disclosure agreement
Threat Intelligence	Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. (Gartner)
RTP	Red Teaming Provider
Availability	Ensuring timely and reliable access to and use of information. (NISTIR 7298r2 Glossary of Key Information Security Terms)
NIST	The (U.S.) National Institute of Standards and Technology (www.nist.gov)
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (NISTIR 7298r2 Glossary of Key Information Security Terms)